SOCIAL MEDIA:
A VALUABLE TOOL WITH RISKS

Major Cities Chiefs Associates
Major County Sheriffs Associates

And

Federal Bureau of Investigation
National Executive Institute
Associates

July 2013

SOCIAL MEDIA
TABLE OF CONTENTS

FOREWORD

The Major Cities Chiefs Associates (MCCA), the Major County Sheriffs (MCS), and the FBI National Executive Institute Associates (FBINEIA) are organizations consisting of Chief Executive Officers of the largest law enforcement organizations mainly in North America. Membership includes departments from the United States and Canada for the MCCA and MCS, and the FBINEIA membership is global. The Human Resources Committee (HRC) of the MCCA, with members from the MCS and FBINEIA, meets three times a year to research, discuss and formulate strategies for contemporary personnel and policy issues and incidences.

The HRC is comprised of individuals, both sworn and civilian professionals, who have distinguished themselves as leaders during their careers. They are charged by their Chief Executive Officers with addressing Law Enforcement's challenges and providing strategic alternatives for implementing, resolving and mitigating human resource issues of today.

Readers of this work will realize how difficult it is for writers to state opinions or make suggestions that apply equally to local, state, urban, rural, suburban, or federal law enforcement agencies. However, the HRC's experienced and wise practitioners are not just espousing theory, but they are actually transforming these ideas into performance on a daily basis. These professionals created this written document from their research, their experience, and from many discussions within the Committee.

While the MCCA, the MCS, and the FBINEIA do not specifically endorse every conclusion or recommendation of this report, they use its information to generate discussion and reasonable debate during their roundtable sessions. The result is better informed Chief Executive Officers who will continue to lead policy changes that will improve law enforcement services.

Companies or individuals identified or cited in this project are not endorsed by the MCCA, MCS, or the FBINEIA, and they are provided for information purposes only.

ACKNOWLEDGEMENTS

The Human Resources Committee of the Major Cities Chiefs and the Major County Sheriffs would like to thank Anna Grymes-Griffin and the FBI Academy for providing lodging, meeting facilities, and administrative help as we kicked off this study. We would also like to thank Miriam Bryant, City of Virginia Beach Human Resources Coordinator and Chief Jim Cervera, Virginia Beach Police Department for their generous hospitality to us in our April meeting on this project.

Recognition is given to the committee members who spent valuable time in travel, research, discussion, writing and editing of this report. While the entire Committee contributed to the project, the following list of Human Resources Committee members and contributors either attended the sessions or specifically worked on the completion of this publication:

Laura Adams	Montgomery County Police Department
Alan Bluemke	Honolulu Police Department
Dwight Bower	Fairfax County Police Department
Miriam Bryant	Virginia Beach Police Department
Jill Celaya	Phoenix Police Department
Tim Collins	Seattle Police Department
Cassandra Deck-Brown	Raleigh Police Department
Frank Domizio	Philadelphia Police Department
Chris Edmonds	Fairfax County Police Department
Jen Ford	Pittsburgh Bureau of Police
Jennifer Greene	Washington D.C. Police Department
Diana Haines-Walton	Washington D.C. Police Department
Daniel Hickson	Washington D.C. Police Department
Ben Houston	San Francisco Police Department
Marty Humphrey	Fort Worth Police Department
Sherry Hunter	Raleigh Police Department
David Jakaboski	Dallas Police Department
Lara Jones	Salt Lake City Police Department
Tom Krumpter	Nassau County Police Department
Ken Lack	Nassau County Police Department
Edward Lang	Philadelphia Police Department
Debbie Langford	Montgomery County Police Department
Mike McCoy	Houston Police Department
Bud McKinney	Strategic Leader, Inc.
Martha Montalvo	Houston Police Department
Patti Moore	Phoenix Police Department retired
Kimberley O'Connell	Chicago Police Department
Vince Robison	Louisville Metro Police Department
Bryan Seboe	Minneapolis Police Department
Jodie Silva	Houston Police Department

Peter Sloly	Toronto Police Service
Andrew Solberg	Washington D.C. Police Department
Martha Stonebrook	Salt Lake City Police Department
Alice Villagomez	San Francisco Police Department
Valarie Williams	Milwaukee Police Department
Regina Woolfolk	Houston Police Department

This publication is available online at the Major Cities Chiefs /National Executive Institute's website: www.neiassociates.org

Chief Jim Cervera, Virginia Beach Police Department, HRC Executive Chairman,
Hugh M. (Bud) McKinney, Senior Advisor, MCCA HRC

INTRODUCTION

Based on the input of the member chiefs of the Major Cities Chiefs Associates (MCCA) and from discussions of the MCCA Human Resources Committee (HRC), there was a perceived need to do a project on social media and its effect on law enforcement. In the MCCA HRC 2011 project on discipline, the subject of social media and the increasing occurrence of abuse and misuse was discussed. Increasingly, over the last two years, law enforcement organizations around the world are using social media as a strategic tool for direct two-way communication. Then in the May 28-29, 2013 MCCA meetings in Grapevine, Texas, Toronto Police Service made a presentation on Social Media and Cyber Security and it all came together.

These two issues together may be the greatest tool and the greatest vulnerability for LE Agencies for the next few years. While you need to deal with both sides of this two-edged sword, this work will be limited to the social media issue. Perhaps the HRC's next study would include the cyber security issue. This study is meant to help edify law enforcement in some of the uses our research has uncovered. To those who are technologically savvy, there may be no surprises, but to others, this may be an opportunity to stretch their paradigm. Those who don't stretch may stay idle at their own peril.

Here is the bottom line up front (BLUP). The BLUP is that you already have the solution to these two critical issues in house. The solution is that there are five to ten "kids" working in your organization that are already using social media extensively and they have ideas how to implement social media to your best advantage. Additionally, you have bright mid-level leaders in your organization who also have a working knowledge of social media. These technologically savvy supervisors can help guide and direct these young resources to keep them from going in too many directions, or on the wrong track. Along with the BLUP solution, now all that is needed is to identify these folks and put them to work on this critical issue.

To begin the introduction of this project, a definition and some examples would be helpful. Social media originated as strictly a personal tool that members used to interact with friends and family. However, law enforcement departments now use social media accounts for a variety of purposes. It now allows anyone with Internet access, including law enforcement, to interact with millions of people online. It provides the ability to disseminate information, as well as personal or professional thoughts and ideas to a wide audience.

Government agencies regularly rely on social media to engage with their customers for improved citizen services and cost savings. Social media integrates technology, social interaction, and content creation to collaboratively connect online information. Through social media, people or groups can create, organize, edit, comment on, combine, and share content, and in the process, help agencies better achieve their mission and goals. The following are the more popular and commonly used social media in government:

Blogs (e.g., WordPress)
Microblogs (e.g., Twitter)
Twitter Town Hall Chats: Best Practices for Federal Agencies
Twitter Town Hall Sample Agenda
Wikis (e.g., Wikipedia)
Video
Podcasts
Discussion Forums
RSS Feeds
Photo Sharing (e.g., Flickr)
Employee Ideation Programs
Gamification
Social Networks (e.g., Facebook)

The top 15 most popular social networking sites according to eBIZMBA as of April 2013:

1 Facebook
2 Twitter
3 LinkedIn
4 Pinterest
5 MySpace
6 Google Plus+
7 Deviant Art
8 LiveJournal
9 Tagged
10 Orkut
11 CafeMom
12 Ning
13 Meetup
14 myLife
15 Multiply[i]

IS SOCIAL MEDIA A DISTRACTION?

Are you a regular user of social media websites and applications? If yes, you are more productive in your work than people who are not. This is the conclusion published in Inc. based on a recent study by the data analysis company Evolv, entitled “Social Media: Not the Productivity Killer You Thought?”[ii]

The basis of the Evolv study and the Inc. article was a survey that focused on the effect that social media websites have on employees. For the purposes of the study, about 100,000 job seekers participated. The analysis found that about 33% of the respondents had between one to four social profiles, about 5% did not belong to any social networks, and there were less than 2% who belonged to five or more social networks.

According to the study, the more social websites an employee used, the more efficient he or she is. The research has found that workers who are socially active on the web, deal with consumer transactions in a time that is shorter and more productive than the average.

But what causes this strange phenomenon for those who use these sites regularly? This study suggests that these people seem generally more social and interactive than others. In addition, workers who have more than one social profile are said to have more experience in technology, which is often a plus for some job positions in today's competitive market.

The report also points out that those who did not use social networks did not stay with the job as long as social website users. However, those belonging to 5 or more social networks also left their jobs quicker. In other words, those on either end of the spectrum, the sticks in the mud and the social butterflies, left their employment more often than those who belonged to 4 or less social networks.

The report offers that for the majority of personnel, the use of social media does not have a negative effect on the employee job performance and productivity. However, they suggest that "before you put a strict social media ban in place at the office—or hire the tech whiz with a following on Facebook, Tumblr, LinkedIn, Twitter, and Pinterest—consider the old adage: Everything in moderation."[iii]

[i] Retrieved online from Ebizmba, April 9, 2013, http://www.ebizmba.com/articles/social-networking-websites

[ii] Retrieved online from Inc. April 27, 2013 http://www.inc.com/francesca-fenzi/social-media-not-the-productivity-killer-you-thought_Printer_Friendly.html

[iii] Id.

SOCIAL MEDIA (SM)
TORONTO POLICE SERVICE (TPS) EXPERIENCE

Document Purpose & Process

This document will present the broad context of SM and the inherent challenges and opportunities for policing in the digital age. The document will also make the case that SM has major global and local impacts. Therefore the information contained herein will have application for all small, medium and large police agencies in Canada, the U.S., and around the world. Finally, the document will use the Toronto Police Service (TPS) as a case study to demonstrate the SM context, challenges and opportunities.

What is the current state of affairs regarding SM in society?

Change is constant. The majority of progress in human history moves in gradual evolutionary change and steady sustainable progress. Technological advances have helped to increase the rate of change in society (the wheel, the printing press, etc.). The Internet and Social Media (SM) have created convulsive, exponential, change. SM is the game changer for “change”!

With the arrival of computers, the Internet, and now SM, the information highway changed technology from dial up to on demand, from linear to network[ed], and from local to global. Information that used to be pushed to the masses through the main stream media on set time lines, now is pulled by users when they want, where they want, what they want, and how they want. SM users drive both demand and supply – content creation is as easy as content access; information analysis is as easy as information dissemination.

It is said that Knowledge is power! SM allows our kids to have the power of the Internet in the palm of their hands with full access to all the accumulated knowledge of human history at the touch of a screen. According to demographers, our kids belong to the “Millennial Generation” (aka Generation Y born roughly between 1980-2000) - this is the largest demographic cohort in human history. Millennials are “digital natives” who were born in the “information age” and who have grown up using Information Communication Technology (ICT) for their entire lives. Millennials are completely comfortable and experienced with SM - they access data, (re)create content and share information with anyone, anywhere, anytime.

SM has enabled mass communication, collaboration and coordination on an increasingly massive variety of digital platforms most of which are free (or ridiculously cheap) and all of which are virtually unhindered by laws, law enforcement, private entities, or nation states. SM is like the “wisdom of crowds” on steroids! Don Tapscott, co-author of the seminal books “Wikinomics” and “Macrowikinomics”, lays out a simple but compelling case that SM is changing mass media and mass communication and massively much more - personal relationships, formal education, private industry, democratic processes, healthcare systems, public safety…everything!

Here are some 2012 SM statistics:

- Monthly active Facebook users is 850 million
- 488 million users regularly use Facebook Mobile
- 17 billion location-tagged posts and check-ins were logged
- 250 million photos are uploaded onto Facebook every day
- If Facebook was a country, it would be the 3rd largest country
- 175 million tweets sent from Twitter every day
- 32% of all internet users are using Twitter
- The average Instagram users spend 257 minutes accessing the photo-sharing site via mobile device.
- The Google +1 button is used 5 billion times per day[i]

SM actually combines the two greatest force multipliers in human history – "social" represents "Human Capital" and "media" represents "Information Technology". Millennial Generation (Human Capital) will use SM (IT) to change the world to a greater, faster, deeper and longer lasting extent than the Baby Boomer Generation!

As an election tool in the political world, SM was a critical success factor used to raise campaign funds, spread their message and to get out the vote. As an adversarial political tool, SM was of critical importance for the people of Tunisia and Egypt to overthrow their nations' rulers. SM was an essential instrument in helping emergency responders in the Haitian earthquake. A person trying to commit crimes on the Internet use SM in a harmful manner and it is being used as a primary instrument for the radicalization/victimization of youth. Whether politically, in business, or socially, SM has been used by many for enlisting help or in the proliferation of misinformation. SM is truly a two-edged sword and can be employed for great good and inordinate evil!

SM requires a new term to be added to the theory of the evolution of species, "Digital Darwinism". Charles Darwin's Theory argued that all species are constantly changing and adapting to survive and thrive. He posited that history has documented in great detail the slow inevitable natural selection of species that live on or die off. Digital Darwinism then, is an attempt to explain the new SM context. The rate of ICT/SM evolutionary change is exponential, and all individuals, organizations, institutions, and nation states have to adapt quickly and continuously or risk extinction. You can't make an "evolutionary" leap across a 20-foot (and quickly widening) chasm in two 10-foot jumps. SM requires everyone to make multiple massive leaps of faith!

Toronto/TPS Context

Toronto is the largest city in Canada (2.6 million people), it is home to the 3rd largest media centre in North America, and it is one of the most diverse cities in the world. The Toronto Police Service (TPS) is the largest municipal agency in Canada (5604 officers), the 4th largest municipal police service in North America, and one of the safest major urban centres in the world.

Toronto/TPS Challenge

Despite Toronto's relatively positive perspective of the city and its safety rankings, the TPS is struggling to provide effective police Service delivery. This is because of the increasingly complex, pluralistic democracy that is itself being radically transformed by the rabid growth of technology and the proliferation and application of SM.

Toronto is also home to one of the largest per capita users of SM in the world, including 4 major universities. Each of these campuses have progressive academic programs designed to provide skilled, accredited ICT professionals for the workforce. The TPS should be able to hire sufficient numbers of police recruits who have the required SM knowledge, skills and experience for the current and future state.

What impact has SM had on public safety and policing?

SM is driving major changes in public safety and police/emergency service delivery. Canadians and agencies around the world are increasingly using SM to address public safety concerns, assess public trust issues and access police services. One of the best examples of public use of social media for public safety is "Ushahidi".

Ushahidi, Inc. is a non-profit software company that develops free and open source software for information collection, visualization and interactive mapping. Ushahidi is Swahili for "testimony" or "witness". In 2007, a young Kenyan man created a website (http://legacy.ushahidi.com) in the aftermath of Kenya's disputed 2007 presidential election. He used this website to collect eyewitness reports of violence sent in by email and text-message, and placed them on a Google map. Ushahidi uses the concept of crowdsourcing in combination with social activism, citizen journalism, and geospatial information. Ushahidi offers products that enable local observers to submit public safety reports using their mobile phones or the Internet, while simultaneously creating a temporal and geospatial archive of events. Ushahidi has subsequently been used in the Haitian earthquake as well as other natural disasters in North America.

The public increasingly expects that the police and other emergency services providers will be using SM to respond to calls for service. In 2012, the Canadian Red Cross commissioned Ipsos Reid to conduct a survey on what Canadians thought about using SM in public safety emergencies:

- 64% of Canadians use SM
- 63% of Canadians expect emergency services to respond to calls posted on SM
- In an emergency 54% of Canadians will use SM to let friends and family know they are safe
- 49% of Canadians said they would sign up for SM electronic alerts in times of official warning.[ii]

Just a few years ago, the vast majority of police leaders saw little value and lots of risk in SM. “Tweeting, following and friending” seemed like the silly talk of teens and eggheads. In that same period of time we have seen how SM has positively and negatively (but always significantly) impacted on local, national and international public safety; the Arab Spring, the UK Riots, the Occupy Movement, lone wolf terror attacks, etc. The “Revolution” may be televised BUT it will be “Tweeted” first! SM is being used by criminals, gangs, organized crime groups and terrorists to commit the full range of public safety threat; flash mobs, on line bullying, identify theft, mass shootings, cyber terrorism, etc. We have seen the direct impact of SM in recent high profile public safety incidents; the Treyvon Martin shooting case, the Hurricane Sandy natural disaster, the LAPD Christopher Dorner manhunt and the Boston Marathon terror attack.

Finally, and not insignificantly, SM has been used to attack the “Police Brand”. There are thousands of viral videos captured by ubiquitous CCTV/PDAs. There are thousands of citizen-journalists capturing every word and action by cops and posting them on blogs. There are thousands of Facebook and Twitter accounts (that reach out to hundreds of thousands of followers/friends) where officer misconduct and misinformation about police agencies are shared 24-7/365/Globally!

SM means there are no more dark places for police officers to commit acts of misconduct, human rights abuses, excessive force or incivility. Everything police do or say will be recorded and posted on SM. The level of police accountability and institutional transparency has significantly increased with SM.

Police leaders are also facing other challenges, like the economic crisis since 2008, the pressure of increased austerity (staffing/budget cuts), the continued loss of police legitimacy/public trust, and the increasing use of SM by criminals and terrorists. The police need to use SM as a force multiplier. The question is no longer whether the police will use SM, it is just how quickly and how well we will do it!

Toronto/TPS Context

In 2009, Toronto was host to the G20. The TPS was challenged with managing both the massive public disorder/riots and the massive media/SM focus on the event.

Toronto/TPS Challenge

In 2009 the TPS had a minimal SM capacity and no formal SM strategy. There were only a handful of members with any SM experience and an operational plan that failed to recognize the need for including SM to support both the public safety and corporate communications strategies. The TPS suffered major public-trust losses as a direct result of the impact of SM.

Toronto/TPS Opportunity

The TPS G20 After Action Report identified the need for a more robust SM strategy that was incorporated into all aspects of core police operations (not just corporate communications but intelligence gathering, crime prevention, public order management, law enforcement, internal affairs conduct investigations and assisting in prosecutions).

How can a police service develop a SM strategy?

Police leaders in Canada and around the world are finally embracing the new SM reality by developing relevant policies, procedures and practices. Police officers are trying to master new technology, new terminology and new rules of engagement. Police leaders are trying to enable and empower their members to close the gap between the current state of SM in society and the state of SM capacity in police agencies. Now there are thousands of official police agency SM accounts in operation across North America and Europe. Many of these police agencies have full SM strategies and/or have members who have become SM subject matter experts. Police Constables are using Twitter to better communicate and collaborate externally with young people and Chief Constables are using Blogs to better communicate and collaborate internally with their employees.

You don’t need to significantly increase your most scarce and most important resources (people, budget and time) in order to create a SM strategy. SM is a high power low cost new tool for police professionals. In fact, any police service that purchases a camera enabled PDA or laptop with internet access has all the hardware/software it needs for a full corporate social media strategy. The next thing that a police service needs is to have an officer who is good at both communication and community policing. Finally, a police service needs corporate leadership - the Chief or a senior officer who will provide the vision, support and resources to enable the front line officer to use SM. Combine off the shelf ICT, a dedicated front line police officer and a visionary police commander then you have all the core elements for a successful corporate SM strategy.

There are three basic SM rules in policing:

1. Police officers hate two things – the way things are and change! Introducing and implementing a SM strategy in policing is always going to be very difficult. SM is not an easy fit in the risk averse, conservative minded, para-military organizational structures/cultures. You need motivated front line officers to use SM, and bold leaders to champion the change. You have to answer questions like "what's in it for me, how much will it cost, will it make cops more effective and the community more safe?"

2. Police can't do SM from behind a desk or through a computer/laptop/PDA! A SM strategy has to focus as much on the "social" (the human element which requires real cops to engage with real community members in real public spaces about real issues) and the "media" (the "information" messages and the "technology" that creates the mediums).

3. Police can't use SM as a silver bullet! Implementing a corporate SM strategy will not solve complex crimes, increase budgets/staffing or improve public trust. A properly implemented corporate SM strategy can enhance police effectiveness in all these areas (and more).

Front line officers are likely to be the first to adopt SM in their daily operations. This is due to the fact that they have the most exposure to the community – specifically to youth in the community who will be the earliest adopters and heaviest users of SM in society. Front line officers will also be the first to realize that criminals are using SM in the virtual world to carry out crimes in the real world. Cops like catching criminals so they will find a way to compete with the bad guys on SM platforms.

Police Chiefs and senior police leaders are more likely to look at the risks and costs associated to SM. To assess and address risks/costs, police leaders need 3 elements in their SM strategy. The strategy must cover 1) governance (to ensure risk management and establish rules of engagement), 2) training (to teach members how to use SM platforms effectively and safely), and 3) evaluation (to identify risks/opportunities and engage in a process of continuous improvement). The problem is that if police leaders focus too much and too early on the "governance" element, the implementation of a SM strategy may take too long and then be too restrictive to be effective.

The rate of innovation and change in the area of social/digital media is "exponential." However, the rate of adoption of SM by police is understandably, but unfortunately "incremental." This has resulted in a growing gap, a gap that consists of a growing list of lost opportunities to leverage SM for improved public safety. It also results in a growing list of SM related threats negatively impacting on public safety.

Toronto/TPS Context

Toronto's large diverse, progressive and creative population has high expectations for its police officers. The TPS has always recognized the need to stay current with changes in society in and information technology.

Toronto/TPS Challenge

The TPS initially resisted using SM. When the TPS started its research into SM we assigned our most risk-averse people to the project (Legal Services lawyers, Professional Standards risk managers, etc.). The TPS was overly concerned with the genuine risks, but largely ignorant of the vast array of opportunities. The early adopters of SM in the TPS were front line officers; Police Constable Scott Mills (the first to use Facebook for youth engagement/crime prevention) and Sergeant Tim Burrows (the first to use Twitter for traffic safety). These front line officers were early adopters/risk takers of SM. Unfortunately, there was little or no buy-in from senior management.

Toronto/TPS Opportunity

The TPS front line early adopters were finally able to convince Deputy Chief Sloly to be there executive champion. Deputy Chief Sloly took PC Mills, Sgt Burrows and the group of risk managers to a SM conference where they focused more on the opportunities than the risks. This event gave each of them a greater confidence in the future of SM for policing. A positive report was given to Chief Blair who approved a full SM strategy for the TPS. The TPS corporate SM strategy was created in six months for $75,000 and now has over 200 trained members using SM (including command officers, front line officers and civilian members).

Can SM improve a police service's corporate communications strategy?

SM had a huge impact early in the area of mass media and mass communication. Community use of SM has rapidly increased simply due to free open source SM platforms. SM use also crosses socio-economic, demographic and geographic boundaries. Consequently, SM has empowered the community to become "citizen journalists" – people whom create/share SM content. That content may compliment and/or critique public institutions like the police. Obviously, police have a global audience and SM active people in the community can post comments to that audience at minimal to no cost, with little or no accountability/liability.

Additionally, traditional communication patterns have drastically changed. Some traditional news outlets have been going under and there has been a decline in advertising revenue as high as 48%. The public increasingly demands more current information and increasingly, they want to be actively involved with decision-making, through collaboration and content creation on those demands. There is an increase in the “micro-online communities” who rapidly and effectively self-mobilize.

From another arena, businesses have been using SM to market, create and strengthen their brands, manage their reputations, and sell their products and services. Traditional mainstream media and corporate communications messages have been replaced by real-time dialogue on SM platforms.

Like most private citizens and businesses, police services have tended to initially focus more on the “media” side of SM. Police leaders have realized that agencies cannot afford to rely on mainstream media and Hollywood to define their brand. Police agencies have come to realize that they can use SM to (re)take control of their messages, to (re)tell their own stories, and to (re)build their own brand!

The police are uniquely well positioned to fully leverage the potential of the new age of SM. They have full access to the two most valuable commodities of the new internet age – “mass information” (policing is a constant source of interesting content) and “mass audiences” (every police agency has its local community as a captured audience). Police have always complained that mainstream media has a disproportionate influence on public perception of police through their potential biases. Now, mainstream media and SM have become the dual prisms whose reflective surfaces portray the police image for the public. The mainstream media filter is no longer the primary definer of police image.

Police can share and receive massive amounts of information with members of the public. They can utilize SM platforms to share public safety information 24-7/365/globally. Police can become the “single source of truth”, the go to place for valid, trusted stats and facts. They can even broadcast their own news - internally & externally. The police can use SM to hold virtual town hall meetings with entire communities and include international participants taking part (with language translation and tools for the visual/hearing impaired). With SM, the police can proactively manage their brand and react in a more timely comprehensive way on what is being said about them (complaints or compliments). Police leaders can now also use SM to reach out to the public and have a dialogue on their own terms in real time/all the time. This is a change to less media relations and more citizen relations.

Internally, SM platforms like blogs and intranets can enhance leadership engagement with employees, cross functional collaboration, and internal information sharing. Externally, SM platforms like crowd sourcing and wiki-processes can improve police-community partnerships, problem solving programs, program evaluation, recruiting/hiring, customer relations' management, and strategic planning.

Not surprisingly, the majority of police services who have established a SM strategy started primarily using SM to enhance their existing corporate communications strategies.

Toronto/TPS Context

Toronto's mainstream media uses police stories for approximately 30-35% of its news broadcasts. Similarly, the 6 million people who live in the Greater Toronto Area (GTA) appear to have a growing appetite for news/information because they are increasingly using SM to receive and share news/information. As a result, the TPS has used its SM strategy to enhance its corporate communications with both mainstream media and direct to our local community.

Toronto/TPS Challenge

The TPS were facing a series of high profile issues like the 2009 G20 Summit, Drug Squad Corruption case, and the Toronto Star Racial Profiling articles, among others. The TPS was also facing significant budget and staffing cuts, while we were being challenged to articulate the value and effectiveness of our police services. Consequently, morale was falling in the TPS and public trust was falling in the community.

Toronto/TPS Opportunity

TPS used its new corporate SM strategy to enhance our corporate communications strategy. We used the TPS corporate SM accounts (Facebook, Twitter & You Tube) to tell our story directly to the people of Toronto - to provide a "source" for relevant police facts/stats. The TPS SM strategy was also used to promote stories about our brave and caring officers, and to market our public safety operations. The TPS SM strategy also signaled that we were a progressive, innovative public institution, capable of leveraging technology to improve effectiveness and reduce costs.

Can SM be used in core police operations?

Given the fact that criminals have been early and effective adopters of SM to carry out a wide and ever expanding range of criminal enterprises, SM can and has to be more than a corporate communications/community engagement tool for police agencies. SM can and should be a core policing tool!

The Police Services Act of Ontario states that the following are the core police service delivery mandates; community policing, crime prevention, order management, emergency response, helping victims, and law enforcement. Police agencies have been able to use SM to enhance each of these areas of core policing.

Community Policing

The police in Manchester, England used SM to "tweet from the beat" in 2010. Manchester was the first major police agency to give PDA's with Twitter accounts to their beat officers with the explicit instructions to send out "tweets" as they patrolled city streets. Tweeted information included proactive patrols of problem addresses, conversations between the officers and the community, and attendance at youth programs. The Manchester police received global mainstream media coverage for this initiative, they significantly increased the number of friends and followers to their SM accounts, and most importantly, public trust and confidence increased.[iii]

Crime prevention

The police in Toronto, Canada use SM to share information with the public regarding crime prevention, loss prevention, and traffic collision reduction. The TPS crime prevention officer of the year in 2012 was PC Ryan Wilmer of 23 Division for his innovative use of SM to enhance his community based efforts. One specific example of how the TPS uses SM to partner with other criminal justice agencies and the private sector is "Fraud Chat" which started in 2012.[iv]

Order Management

The police in London England used SM (Twitter, Facebook, etc.) during the UK riots of 2011. Anarchists and criminals used SM to promote disorder and brag about their criminal acts, which fueled the riots. The London Met and the people of London in turn used SM to identify instigators, prioritize threats, deploy resources, gather evidence, help victims, organize clean ups, and prosecute criminals.[v]

Emergency Response

The police in Groningen, Netherlands created a SM based project called "COMPRONET" which started in 2011. The project allows Dutch citizens to register for a police "app" utilizing Twitter, and allowing them to receive information about public safety emergencies or crimes occurring in their area. The citizens can then use their personal PDA's to gather and share information/evidence with responding police officers in real time about those events (photos of suspects, license plate numbers, suspect direction of travel, victim injuries, etc.). Officer Elle de Jong is the project lead for COMPRONET.[vi]

Helping Victims

The police in Vancouver, Canada used SM to support victims in the aftermath of a major riot. The riot occurred after the local hockey team lost the Stanley Cup finals in 2011. During the riots many people and businesses were victimized – the Vancouver PD were themselves victims of property damage (police cars vandalized) and personal injuries (police officers attacked). The citizens of Vancouver and their police department used SM to identify hundreds of criminal suspects and riot instigators. SM enabled the Vancouver PD to bring these people to justice and to get restitution for many victims. The Vancouver riot victims (the public and the police) were able to use SM to help themselves![vii]

Law enforcement

The police in Philadelphia, PA, use SM to post photos and information about persons wanted in the city. This use of SM has significantly engaged large numbers of city residents in the active pursuit of criminals. The Philadelphia PD has arrested hundreds of wanted parties. The evaluation of this project (and similar other projects in North America) shows that posting information about wanted parties on SM actually increases the likelihood of arrest rather than through the use of mainstream media and more traditional police methods.[viii]

In all of these examples, SM presents an increased risk and an increased opportunity. It is also important to note that in all these examples it is BOTH the police and the public using SM to co-produce better public safety outcomes.

Every crime prevention officer, youth bureau officer, criminal investigations officer, intelligence officer, or public order commander worth their salt is capable and must be using SM to enhance their effectiveness. In fact, SM has assisted police services in missing person searches, rescue/recovery operations, internal affairs investigations, gun/gang/drug investigations, covert operations, intelligence gathering, sexual assault investigations, homicide investigations, terrorism operations, and others. The applications of SM in public safety are only limited by the imaginations of police officers, community members and criminals.

Toronto/TPS Context

Toronto has experienced high profile public safety events where SM was a critical component. These events include Occupy Toronto and the Danzig/Eaton Centre mass shootings. Toronto residents are also increasingly trying to contact police and access police service delivery via SM.

Toronto/TPS Challenge

The TPS made a specific decision to limit the corporate SM strategy to corporate communications and community engagement. The TPS quickly realized that hundreds of police officers were using SM in their investigations. We also realized that our current CAD/communications system was not able to handle SM calls for service. Next Generation 911 is still years away from actual implementation but Toronto residents are not waiting for it – they are calling on SM and expecting us to respond.

Toronto/TPS Opportunity

The TPS made the decision to expand the SM strategy to include core police operations. TPS has used SM analysis to identify criminal networks, created training for detectives, used SM to recover stolen property, arrest wanted suspects, included SM monitoring in intelligence gathering projects, deployed SM officers for public order events, utilized SM in covert operations, brought cases to court with SM evidence, assigned all Neighborhood officers with PDA's to tweet from the beat and is in the process of implementing virtual patrols to augment foot patrols. The TPS also expanded the ability for communications operators to dispatch to SM calls for service (1188 calls in 2012). The TPS has SM integrated into all of its guns, gangs and drug operations and its crime management centerpiece, the Toronto Anti Violence Intervention Strategy (TAVIS).

How do police decrease the risks and increase the reward of SM?

Like all major technological and societal changes, there are great risks. Likewise there are potential hazards for SM in policing.

External Risks For SM In Policing

As discussed earlier, there is an increased expectation from the public for the police to respond to SM calls for service – for both emergency and non-emergency issues. If an officer hears someone yelling for help from inside a building can the officer ignore the call because it did not come through the CAD/dispatch system? Equally, can a tweet for help be ignored if it doesn't come through a 911 line? SM has increased the effectiveness/profitability of criminal enterprises and enhanced the ability of terrorists/anarchists to create public disorder while also creating new types of crime/victimization. Therefore, police must use SM to combat that increase. Can a police agency respond to, investigate and prosecute criminal offences that are carried out almost exclusively over the Internet and SM platforms (cyber bullying, frauds, etc.)? The answer is police agencies must mitigate such liabilities by finding ways to validate all such calls for service (calling 911, yelling for help and SM postings).

Police must create new public and private sector partnerships to accelerate the research and development of the Next Gen 911 technology and related business processes to meet the increased number and variety of demands. Police must also work with elected officials and the courts to create new laws locally, nationally and internationally that will better enable people to use SM and the Internet in a safe, profitable, legitimate way. These same laws must also enable the police to maintain public safety on the information highway.

Internal SM Risks

Some members are using SM inappropriately in their professional and personal lives. This tarnishes the reputation and that of their police department. The prevailing practice when it comes to member misconduct via SM is to create specific rules for SM misconduct. This goes against the prevailing wisdom. Common sense and common decency should tell officers that they can not post a racist comment on their personal SM accounts, or they can not disclose public safety information on a SM platform. They can not air their personal beefs about their supervisor on an official police service account, and they can not spend their day surfing on SM when they are getting paid a good wage to do an important public safety job. The officer's oath of office and oath of secrecy coupled with the police agency's core values, performance management systems and conduct governance should already be sufficient to cover SM conduct or performance issues.

Police agencies with SM strategies need to reinforce existing governance with some SM specific procedures and training which shows members how "regular" conduct/performance issues can be affected with SM.

The other area of risk relates to how SM interfaces with the police and the rest of the criminal justice system. Police are now using SM as an investigative tool – we are monitoring open source SM communications. We are gathering digital evidence that is both open source and private, and we are involved in covert operations using SM, etc. There is significant evidentiary value in SM information, and SM is increasingly relied upon to form our reasonable grounds for belief and varying degrees of foundation for search warrant applications.

Ultimately, all SM information gathered must be considered as subject to disclosure to a variety of public forums including but not limited to civil, criminal and federal courts, as well as human rights tribunals, police oversight bodies, etc. As such, SM information needs to be managed following similar standards currently adhered to today for physical "evidence" (biological, digital, photographic, video and audio evidence). Standards in regard to format, presentation and storage need to be established based on the type of SM data being seized.

- Intelligence information gathered from SM requires more storage, new search and retention capability, format standardization, packaging, presentation, etc.
- Current legislation relating to information privacy, IP addresses, lawful access needs to be both adhered to and while new legislation is created and enacted
- Courts (judges, lawyers, etc.) have to be educated on SM and their input has to be sought to ensure acceptance and process
- Evidence continuity for digital content is also a consideration – from crime scene management, to court disclosure and return dispositions for the original owner
- Defensible processes will ensure reliability of evidence, maintain credibility in the process, and mitigate risk

Policing is a business - we are in the business of improving public safety, public service and public trust! SM is not a panacea to fix all of what ails policing, nor is it a threat to good policing. The challenge for business leaders and police leaders is to minimize the risks and maximize the rewards of SM. There is no doubt that it is a powerful new business/public safety tool that will help committed police leaders, courageous front-line cops, and good community partners to better communicate, collaborate and co-create public safety. Implementing a SM strategy is difficult in policing but it must be done and it can be done.

Toronto/TPS Context

Toronto, Canada is a city but it is also part of inter(net)connected global village. The Internet connects everyone in Toronto to everyone else in the world through in a virtual world where there are few laws – there are no rules of the road on the Internet Super Highway.

Toronto/TPS Challenge

The TPS needed to address the risk of community members using SM for calls to the police for help, criminal members using SM for illegal activities and TPS members using SM for unethical conduct. The TPS did not have the capacity to address these problems – there are only a few recognized TPS SM experts. The TPS also had to work within the Canadian criminal laws and the TPS governing laws that may not be able to address the new SM enabled world.

Toronto/TPS Opportunity

The TPS accelerated its SM strategy by contracting/partnering with private entities. The TPS used private consultant Lauri Sevens of Laws.com to develop its corporate SM strategy. The TPS has also partnered with SM subject matter experts (SME) like Don “Macrowikinomics” Tapscott to educate its senior managers on the SM risks/rewards. The TPS has partnered with private companies like Microsoft Canada to design a new Duty Operations Centre that will be capable of receiving, validating, analyzing, and responding to SM calls for service along with advanced SM monitoring. The TPS is working with government officials and justice officials to create the framework for a provincial e-Disclosure system that will allow police to gather, store, disclose and present digital evidence in cases. Finally, the TPS is assisting the Canadian Association of Chiefs of Police to advocate for enhanced and new laws that provide lawful access for the police to access info on private IP addresses through Telco providers.

What does the future state of SM in policing look like?

Globally, we are going to see a further and faster growth in the use of SM and digital platforms. There will be an app for everything you can think of! The rate of change will increase, the SM risks/rewards will increase and the gap between current police SM capacity and community expectations of police SM capacity will increase.

Community members and criminals will continue to be early adopters of SM related technology for good and bad purposes. Police officers and civilian members will increasingly need to use SM to “get the job done”. Police leaders and police oversight bodies will be expected to leverage SM to reduce costs, increase efficiency, and improve accountability.

Then there is the real and present danger posed by cyber threats. This is a topic unto itself, but suffice it to say, the threat continuum ranges from teenaged mischief making hackers joy riding on the Internet, to organized crime syndicates, terrorist groups, and powerful nation states who use SM to finance and wage cyber wars. Right now criminals operate in the “deep web” using cheap “apps” to build “bot nets” to mine “big data” in order to create untraceable “bit coin” fortunes to fund further illegal and unethical activities! If those terms are confusing to you, you are not alone. Google glasses, in combination with advanced facial recognition software in the hands of a criminal, could compromise officer safety and undermine most police covert operations. If this worries you, then you are paying attention! Anonymous is a loose but formidable network of “hacktivists” who can combine their considerable SM SME capacity to “virtually” and physically intervene in any public safety/political event! They accomplish this through hacking private corporations, shutting down public institutions systems, and exposing institutional weaknesses. If the above seems amusing, it shouldn’t be! Lastly, a teenager developed an app that can allow anyone to take over the flight controls of a commercial plane – this is 911 on SM! If that scares you, it should!

In the near future, the police must try to better communicate and connect with the public using different SM platforms to create public trust while increasing public safety and the perception of safety in the community. Not just in the real world but in the SM world too.

SM sites like “Second Life” engages hundreds of thousands of people in a virtual world where they can live out any fantasy they want for a small price which generates billions of dollars for the creators of the SM platform. In some cases, people are more attached to their “second life” than their real life. Given the popularity and power of such SM platforms you can see why futures theorists like Professor Sohail Inayatullah predicts that the police will have to physically patrol the “beat” and also patrol the digital “beat”.

The future is now! In fact, police can patrol the digital SM beat right now by checking-in to locations using Foursquare, taking photos and uploading them onto Instagram, answering questions on Twitter, engaging youth on chat sites, intervening in cyber bullying, and educating parents on how to keep their families safe on the Internet.

Clearly, SM is no longer a passing fad or a new medium for corporate communications, but a “whole of agency” issue, an operationally necessity and a new core policing competency. As with scientific advances such as fingerprints, forensic sciences, and DNA that have assisted law enforcement in solving crimes, the era of SM is the “next big thing” in policing.

So how can police leaders close the SM gap, mitigate the ever-increasing SM risks, and more fully leverage the SM opportunities? It’s not more IT – it is more HR. People are the key to success! Our best hope lies in the hardworking, dedicated police officers and civilian members who have been and will continue to be the greatest force multiplier for police services.

The good news is that if your police agency has been hiring recruits, then you will have a fresh stock of highly SM competent “millennials” who grew up entirely in the information age. These millennials are inside your police agency, but you have to find them, and engage them in creating/implementing/leading your corporate SM strategy. Leaders must empower them to be innovative, provide them with regular feedback and informal rewards, and retain them by continually giving them new challenging assignments. That is a list straight out of how to manage millennials. These SM savvy employees will be the best police SM change champions.

Every police agency has to revisit their list of core competencies, update their desired knowledge/skills/aptitudes, enhance their talent management programs, and create human capital strategies to ensure that there is a focus on SM. Police leaders must hire, develop, promote, and retain tech savvy, SM SME’s in significant numbers.

Police agencies that can combine solid IT SM strategies, with innovative HR SM strategies and broad operational SM strategies will be the future of policing in a SM dominated world.

Toronto/TPS Context

Toronto has benefitted from its ability to leverage IT and use SM in innovative ways. Toronto is also home to world renowned SM SMEs. But Toronto has also seen its share of hacking incidents and Torontonians have been victimized by bot nets, identity thefts and corporate espionage.

Toronto/TPS Challenge

The TPS has to be able to serve and protect its million of residents in both the real and virtual worlds. As the economic powerhouse for Canada, Toronto is a rich target for hackers, criminals, anarchists and terrorists who want to use SM for evil. So the TPS has to be up to the emerging SM challenges.

Toronto/TPS Opportunity

The TPS has hired over 2000 new members since Chief Blair took office. Most of those new employees are part of the millennial generation. Ritesh Kotak, a classic Millennial, is a Parking Enforcement Officer who had less than 2 years of employment with the TPS. In 2012, Deputy Chief Sloly discovered this SM genius writing parking tags. Deputy Chief Sloly recognized his massive SM talents and seconded him to review the TPS corporate SM strategy.

Under Chief Blair's direction, the TPS has created a special project team called "Operation Re-Boot". Ritesh Kotak is coordinating the project that includes some of our most experienced but progressive senior officers along with some of our most innovative millennial members. The goals of Operation Re-Boot are identifying and testing new IT/SM applications, developing a cyber risk strategy, and leveraging existing/emerging ICT. In the 12 months since then, Ritesh Kotak has reviewed, rebooted and revolutionized the TPS SM strategy. Subsequently, Deputy Chief Sloly and Ritesh Kotak have presented “Operation Re-Boot” to PERF and MCC as an emerging best practice for SM in police.

Key Players

The following is a list of potential key players;

1. Police Service Boards
2. Police Associations
3. Public Safety Canada
4. Provincial & National Privacy Commissions
5. Telecommunications Companies (Rogers, Bell, Telus, etc.)
6. Social Networking Sites (Facebook, Google, Twitter, etc.)

7. Recognized SM subject matter experts
8. Crown Prosecutors, Defense Lawyers & Judges
9. Canadian Radio & Television Corporation
10. Private Citizens/Public

Key issues

The following is a list of key issues:

1. Educate police leaders on the role of SM in policing & public safety
2. Create a basic SM governance framework for police agencies & oversight bodies
3. Establish ongoing surveys of public & police SM expectations/needs
4. Create list of existing SM related legislation & advocate for new legislation
5. Include SM as a strategic priority for police agency IT/ICT strategies
6. Establish both operating and capital budgets for improving SM capacity
7. Update HR strategies for police members to improve SM competency
8. Identify SM best practices, emerging technologies & potential application
9. Assess the potential cost benefit analysis for use of SM in policing
10. Involve community, private industry & academics to develop SM in policing

12 Month Plan

1. Create initial Scope Document for 2013-02
2. Create initial FAQ Document for CACP Annual Conference in 2013-03
3. Create full Sub-Committee involving key players (identified above) for 2013-04

International / National / Regional / Local Perspective

SM has international, national, regional and local impacts. Every Canadian community accesses and uses SM, and all aspects of Canadian society uses SM, with increasing frequency. Therefore, every police agency in Canada needs some level of SM capacity (small/medium/large, municipal/provincial/federal or rural/urban/Aboriginal).

Given that Canada is a nation of immigrants, that criminals operate without regard for jurisdictional/geographic boundaries, that police operations increasingly involve the Internet/SM, and that we live in an increasingly globalized world, then all police agencies need to increase their SM competency and capacity.

The main challenges to fully implementing a SM strategy for the CACP member agencies will be provincial, federal and international legislation – complying with existing legislation and creating needed new legislation.

Date of Report
2013-07-13

Strategic Objective
Social Media (SM)

Team Lead and Team
Team Lead
Peter Sloly – Toronto Police

Team
Brendan Dodd – Windsor Police
Eldon Amoroso - CACP
Lance Valcour - CITIG

[i] http://www.huffingtonpost.com/brian-honigman/100-fascinating-social-me_b_2185281.html, retrieved from the Internet 6/28/13.

[ii] http://redcrosstalks.wordpress.com/2012/10/09/tech-talk-canadian-survey-on-social-media-in-emergencies/, retrieved from the Internet 6/28/13.

[iii] http://www.guardian.co.uk/uk/2010/oct/14/manchester-police-twitter-experiment, retrieved from the Internet 6/28/13.

[iv] http://www.torontopolice.on.ca/newsreleases/pdfs/26706.pdf, retrieved from the Internet 6/28/13.

[v] http://www.bbc.co.uk/news/uk-politics-14931010, retrieved from the Internet 6/28/13.

[vi] http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=2356&issue_id=42011, retrieved from the Internet 6/28/13.

[vii] http://www.vancouversun.com/news/Vancouverites+fight+back+against+rioters+through+social+media/4958109/story.html, retrieved from the Internet 6/28/13.

[viii] http://www.nbcphiladelphia.com/news/tech/Philly-Police-Solving-Crimes-With-Social-Media-Help-147383265.html, retrieved from the Internet 6/28/13.

SOCIAL MEDIA USES FOR LAW ENFORCEMENT

Administrative Uses: Recruiting, Community Outreach, Press Release, and Public Feedback

Social media networks are used by many agencies to advertise current employment opportunities, specify employment qualifications and hiring requirements, list information pertaining to salary and benefits, announce dates for testing, and to advertise departmental information sessions. By linking the site to an agency's webpage, applicants are able to view pertinent information such as recruitment videos, employment applications, and peruse the agency's hiring process.

Social media can be also used as a tool to strategically attract groups that are underrepresented in law enforcement. Advertising via social media networks and participating in community events such as career fairs, sporting activities, cultural festivals, school activities, collegiate presentations, etc., may provide exposure to the law enforcement profession for female, minority, or ethnic groups to better reflect an agency's population.

Recruiting through social media requires a smaller monetary investment as compared to television commercials, radio ads, billboards and career fairs. Its use in private industry is commonplace. Jon Hull, head of resourcing at the electronics and maintenance distributor RS Components said, "As well as reducing the cost of recruitment by over 50%, social media also significantly reduced the number of man-hours needed to identify suitable candidates. Social media delivered an average time-saving of four hours per candidate for the line managers involved and over seven hours per candidate for our in-house recruitment team." [i]

Governmental agencies regularly rely on social media to engage with their customers for improved services and provide cost savings. Social media integrates technology, social interaction, and content creation to collaboratively connect online information. Through social media, people can create, organize, edit, comment, combine, and share content to aid agencies in achieving their mission. Examples of this process in law enforcement include Crime Stoppers tip lines, Missing Persons Alerts (Amber and Silver Alerts), crime alerts for serious offenses, press releases, departmental accolades, positive news stories, and community events. In addition, through social media networks, citizens are able to provide feedback by posting comments and concerns to their local agency.

In short, social media sites provide an avenue to produce responses to situations that require immediate attention or can be intended to reach a large audience. An agency's Public Information Office is instrumental in facilitating this process by means of social, broadcast and print media. As a model, the Public Information Office (PIO) serves as the liaison between the Department and the members of the local, national and international media. The PIO is responsible for the release of accurate and timely information regarding the activities of the Department to the news media and the public. The function of PIO is an integral component of the day-to-day law enforcement operations of the Department. One of the goals of the PIO staff is to make sure the avenues of communication are consistently open among the Department, the media and the citizenry. The rapport established between the PIO staff and the media benefits both entities. The media receives extremely current and factual information for publication and broadcast, while the law enforcement community benefits from the media's enhanced dissemination capabilities to publicize the Department's crime prevention efforts, as well as the community policing projects. The PIO should strive to promote a positive image of the department through its relationship with the media outlets, and facilitate specialized programs tailored to the needs of the community.

Social media networks are often used by agencies to disseminate information to and receive information from employees and the public. Examples include messages from the Chief, press releases, neighborhood crime alerts, GovDelivery,[1] and links for reporting illegal activity. All sites should be monitored for inappropriate comments (hate speech, profane and vulgar language) and replies should be provided for posts that require a follow-up response.

Social media have given recruiters a larger number of tools to use in identifying, recruiting, and hiring the right candidates. Social media has also provided a means for law enforcement agencies to get their messages out, unfiltered and not translated through media bias. Because social media gives LE the ability to go directly to the targeted audience, it also encourages the participation of public media in getting these messages to the communities.

> Social media is emerging as a tool that more recruiters rely on in the hiring process. Networks such as LinkedIn, Facebook, Twitter, Viadeo, and Google+ can provide recruiters with an array of information about potential candidates, as well as new avenues for reaching passive candidates and advertising the [agency's] current openings.[ii]
>
> …As a recruiter, you want to be where the most qualified, talented, and largest pools of applicants are. Human resources can leverage social media to tap in to potential recruits. This type of head hunting is called social recruiting. It's about engaging with users and using social media tools to source and recruit talent.

[1] From their advertisement - **GovDelivery** is the leading public communication solution, offering an automated Email and Digital Subscription Management platform to government.

LinkedIn, Facebook, and Twitter have over 535 million combined users. That equals a lot of potential talent for your company (agency).[iii]

Recap Bullet List of Social Media Uses for LE

The following is a list of some of the ideas on uses of social media for a law enforcement agency:

* Use social media to advertise all aspects of upcoming test dates

All advertising should have a common theme that includes a common message. Upcoming test dates should be included in virtually all department advertising. PR group should prioritize the recruiting message within the space allotted for each of the ads.

* Pre Workshop Entry Test

Pre-workshop classes are to be treated differently than test dates. Pre-workshop classes can be heavily promoted in the underrepresented target groups that the dept. would like to increase representation of a specific group.

Pre workshop classes can be used for Police, Parking Enforcement, and Dispatchers.

* Use social media to link hyperlinks to Agency webpage

Add tag lines to all traditional advertising to complete the recruiting circle. Tag lines could be added to billboards, radio ads, and broadcast spots.

* Evaluate social media effectiveness monthly for appropriate calibration

Social media websites count specific "hits" to it's website that logs the number of visitors. Hits can be measured against peer departments for effectiveness. Defining effectiveness would be hard to judge because of the pervasiveness of why individuals use social media. Tracking data can fall into multiple categories such as Traffic data, Fan following data, Social interaction data, etc. Police work might gauge overall traffic data because of the specific reason our customers visit Law Enforcement sites.

* Targeted Advertising - Groups underrepresented in the law enforcement agency could garner a specific recruiting strategy that would be more receptive to their frame of reference. Recruiting strategies could include adding a social media presence to events dealing with targeted groups such as: Cultural advertising, fun run's, school activities, career fair ads, sporting events, etc.

* Low Cost Recruiting

Recruiting on social media requires a much smaller monetary investment as compared to commercials, radio ads, billboards, and Career Fairs. This lower investment allows funds to be diverted in other areas within the agency. Most costs include up to date computing equipment, an ergonomic seating environment, and man-hours to provide content. Additionally there will be specific software requirements that match the mission of the campaign.

[i] Hull, Jon, hrmagazine, *50% reduction on recruitment costs*, April 27, 2011, Accessed April 8, 2013. http://www.hrmagazine.co.uk/hro/features/1019381/-reduction-recruitment-costs-social-media-friend

[ii] Fort, Judy, HR Smart, *hrsmart.com*, February 18, 2013. Accessed April 8, 2013, http://www.hrsmart.com/blog/role-social-media-recruiting.

[iii] Black, Tiffany, Inc., *How to Use Social Media as a recruiting Tool*, April 22, 2010, Accessed April 8, 2013, http://www.inc.com/guides/2010/04/social-media-recruiting.html.

Using Social Media To Determine Suitability of Police Officer Candidates: Proceed Cautiously

According to Jonathan Hyman, author, attorney and partner in the Labor and Employment Group at Kohrman Jackson & Krantz in Cleveland, Ohio, 91% of employers use social media to aid in their decisions of who, and who not, to hire."[i] While this practice is becoming increasingly common, law enforcement agencies have only recently begun to make use of social media sites as one of the resources for conducting comprehensive background investigations of applicants for police officer positions. Traditionally, applicants for police officer positions complete a multi-page booklet that queries the applicant on many areas including employment, education, residency, personal character, professional references, the applicant's criminal and civil litigation history, credit, military and a host of other areas. Applicants complete the booklet and sign waivers authorizing the agency to verify the information in the booklet by examination of documents, face-to-face interviews of references and, examination of public records such as civil court and criminal records. While the applicant has no control over what is told to the pre-employment investigator by references, the applicant has provided the information that forms the basis of the background investigation. In this sense, the applicant maintains a modicum of control over the investigative process.

Unlike traditional information gathering through verification of documents and information provided by the applicant, the use of social media sites as an investigative tool presents a method of pre-employment investigation that may be totally out of the control of the applicant. While a law enforcement agency would be remiss if it did not access social media sites to learn more about the applicant, the applicant has no power over the information in cyberspace. The inability of the applicant to control information that is placed on the Internet, including information placed on the applicant's own personal webpages, is a good reason for law enforcement agencies to use social media sites as one of several tools to investigate the suitability of applicants. However, no decision should be made on the suitability of applicants based solely on what has been gleaned from Internet social media sites.

When conducting a background, what can a law enforcement agency expect to learn about an applicant using social media sites as part of the background investigation? "…[A]n employer can learn that a candidate lied about his or her qualifications, posted inappropriate comments, trashed a former employer, divulged corporate confidential information, or demonstrates poor communications skills." [ii] Any one of the above "could legitimately disqualify the candidate from further consideration. Conversely, an employer can discover that a candidate is creative, demonstrates solid communication skills, received awards or accolades, or is well regarded or recommended by his or her peers.[iii] Clearly, using the information on a social media site as the primary reason in making an employment decision carries some risk. "Despite the legitimate information an employer can discover"[iv] about job applicants through social media and other websites, conducting such informal Internet background checks should proceed cautiously because of the risks. First, information uncovered through Internet social media may be "unreliable and unverifiable."[v] Further, there is a genuine risk that an Internet search will disclose "protected information such as age, sex, race, religion, or medical information."[vi]

For these reasons, law enforcement agencies should establish clear policies on when and under what circumstances social media sites will be used during the background investigation process. The social media protocol should be developed in consultation with agency counsel, the Ethics Officer, and the Public Information Officer. Together different units in agencies can develop policies and procedures for the obtaining and the use of Internet-based information without conflicting with privacy, discrimination, and other laws. Additionally, agencies should:

- Include on the job application a statement that Internet searches may be conducted for publicly available information, either through social media sites or through the use of search engines. The point is to obtain the applicant's signed permission to conduct the search.

- Web searches should not be done before making a conditional job offer to the candidate.

- The use of a third party vendor specializing in background searches may be considered to do the searching, but with instructions not to disclose to you any sensitive or protected information that may be uncovered.

- Obviously, Internet searches are only one of several tools to use in background screening, in order to gain the most complete and accurate picture of the applicant.[vii]

The Recruiting Division of the District of Columbia Metropolitan Police Department established a comprehensive protocol for the use of Social Media as a background investigation tool. Special Order 13-03, establishes social media sites as a viable background investigation tool. It sets forth a clear policy of the risks and benefits of using social media to determine suitability of police officer candidates. The policy also provides clear guidelines to background investigators on how the information can be accessed, reviewed and considered in the hiring process. Finally, the order establishes a neutral third party as the person responsible for accessing the social media sites and providing the information to the pre-employment background investigator. Additionally, this third party does not make the employment decision, nor do they determine what is to be included in the comprehensive investigative report.[viii]

The Major Cities Chiefs departments are not alone in using social media sites as one of their investigative tools for determining suitability of applicants for police officer positions. Medium and small agencies should be and many already use this tool. Before hiring a new sheriff's deputy the Sheriff of Gloucester County, Virginia, directs the investigator assigned to the case to probe the job candidate's social media pages, checking out his friends, pictures and posting.[ix] In fact several law enforcement departments throughout the Commonwealth of Virginia use social media during the vetting process.[x] But there is a caution not to overreach because there have been instances of pushback. In 2012, the Virginia American Civil Liberties Union sent a letter to the state police superintendent questioning the Virginia State Police practice of having prospective troopers sign into their social media profiles on an agency laptop to allow a background investigator to look at it.

In closing, if law enforcement agencies avoid social media sites altogether, they may be missing opportunities by not taking advantage of this potentially valuable information. However, agencies will want to minimize their vulnerability to lawsuit or bad press by establishing clear policies. Policies similar to the one implemented by the DC Police Department can help mitigate against these problems. Agencies need to understand that employment decisions based upon information gained through an applicant's social media site is not without risk. If the employer takes the appropriate steps to minimize that risk, and conducts the social media search in accordance with all federal, state and local laws, social media checks may be a valuable tool in the hiring process.

[i] Hyman, Jonathan T., 2012*The Employer Bill of Rights: A Manager's Guide to Workplace Law*, p 21. Springer-Verlag, NY, NY.

[ii] Id., p. 21.

[iii] Id., p. 21.

[iv] Id., p. 21.

[v] Id., p.21

[vi] Id., p 21.

[vii] Id., p 22.

[viii] *Social Media Checks for Background Investigations*, SO-13-03, April 2, 2013, District of Columbia Metropolitan Police Department, "*Labor: Should You Use Social Media To Screen Job Applicants?"* http://www.insidecounsel.com; February 11, 2013.

[ix] "***Public Safety Agencies Use Social Media To Check Applicants' Backgrounds"*, The Daily Press, September 1, 2012,** Tyra M. Vaughn, http://articles.dailypress.com/2012-09-01/news/

[x] James City, Hampton and Williamsburg Counties all access social medial sites to review applicants' social media pages and determine whether derogatory information exists that would deem the applicant unsuitable for a public safety position., ID

Use of Social Media For Criminal Intelligence Gathering and in The Investigation of Police Misconduct (Internal Affairs)

Social networking has become a valuable intelligence-gathering tool for law enforcement agencies. It is also a source of evidence for defense and prosecution personnel. A search of Facebook pages, Twitter feeds or YouTube videos can provide evidence to discredit witnesses, establish either pro or anti law enforcement bias, to track down evidence, or to establish associations between gang members. Often, perpetrators brag about their crimes on social networks, and child pornographers and sexual predators have been located and apprehended as a result of their online activities. Police Departments use social media platforms to broaden information gathering and to leverage public support. Both lawful citizens and criminals are voluntarily posting more and more information online. Because it is easily accessed, it can help in putting together a more comprehensive investigation for prosecution or defense. Videos that are posted of parties, social gatherings, or even criminal behavior allows law enforcement to

> "put faces with street names and put people in association with others, when you ordinarily wouldn't be able to do that…Even five years ago, if you wanted to show an association between two people, you had to do surveillance. Now you can just go to blogs, video or image sharing sites, and in many cases, find those pictures."[i]

The use of social media for intelligence gathering by law enforcement agencies is perhaps one of the most popular uses of social media by law enforcement personnel. The ability to glean information on suspects by combing through publicly available Facebook pages, blogs, YouTube videos and other sites have provided law enforcement agencies across the country with invaluable information on past crimes, current investigations and conspiracies to commit crimes. Many law enforcement agencies embrace the use of social media as an investigative tool because it doses not require search warrants or wiretapping to find valuable information. For example, criminals sometimes think they are anonymous when online. Seattle PD had a case where a prolific motorcycle thief used a Facebook page. The investigators accessed the thief's Facebook page, and saw that he had posted photos of himself on stolen motorcycles. Using the information from Facebook, they were able to get not only the conviction of the thief but also the arrests of the proprietors of chop shops used by the thief.

This is an example that demonstrates how law enforcement has used social media to assist in their investigations. However, the caution on using social media as the sole source for determining suitability in a background investigation, applies to the use of social media as a criminal intelligence-gathering tool. Social media is best used in conjunction with traditional methods of investigating criminal activities. There are pitfalls of using social media in criminal evidence gathering. The major pitfall has been the ability to keep, maintain, and authenticate records that have been produced through the use of social media. Blog notes, videos, web pages change in real time. Unless the law enforcement agency has established a mechanism for the retrieval, inventory and authentication of the information gleaned from social media, the use of the information in a future trial may prove unreliable.

To reemphasize the above assertions, it is wise to take the time to identify the pitfalls of using social media as a criminal information-gathering tool. Similarly, an agency should develop a solid standard operating procedure on how social media will be integrated in the investigative process. This will increase the chances that the agency's efforts will be sustained in a subsequent criminal proceeding.

The DC Metropolitan Police Department's Criminal Intelligence Unit regularly uses social media to monitor gang activity. The department's success can be attributed to the development of social media teams and the establishment of rules of engagement related to the use of social media. When using social media in intelligence gathering, it is important to:

- Establish the purpose or mission of the use of social media and ensure that all team members understand the same

- Exercise care and ensure that the activities of the team protect person's constitutional rights, and that matters investigated are confined to those supported by a legitimate law enforcement purpose.

- Have a policy where members observe and monitor social media websites that are open to the public, with no invitation, approval or membership required

- Have a policy in cases where it is suspected that a social media website contains posts related to criminal activity or criminal associations, team members must obtain written authorization to join the site. This allows the department to weigh the pros and cons of accessing the site and also integrate traditional intelligence gathering tools to supplement the information from the social media site.

- Have a policy where members maintain records detailing the information disclosed including the identification of the social media site where the information could be found.[ii]

Research did not yield information for the use of social media to lodge complaints against officers, resulting in an investigation by the Department's Internal Affairs Division. There was nothing found on the affirmative use of social media as an investigative tool by Internal Affairs Offices. Most law enforcement agencies' Internal Affairs Units receive information via social media sites that form the basis of investigations of police misconduct. Commander Chris Lojacono, Director of

Washington, D.C. MPD's Internal Affairs Division, said that IAD doesn't normally search social media unless it is part of an allegation against one the employees. However, there have been allegations from others such as the Public Defenders Service who have searched social media on employees and found inappropriate information connected to that employee. MPD policies caution employees that there are various people who are monitoring social media and employees need to make sure they are not putting out information that could be considered inappropriate conduct or material. To that end, social media can be a negative for employees when it comes to Internal Affairs investigations. In fact, employees' inappropriate use of government computers and mobile devices to access social media while on duty is one of the major areas that would require IAD officials to access social media sites. Therefore, when an alleged violation is reported, the department should monitor any anti-agency sites for negative agency messaging.

There have also been instances when employees have used social media sites to post negative messages about the agency. Therefore, while using the information in an investigation is applicable, the agency should also respond when appropriate to give the agency's message or perspective on a negative misleading post. Generally speaking, IA should not use social media aimed at "fishing" for information unless there is an indication of employee misconduct. It may be suitable for its use to confirm allegations of wrong-doing, but consultation with legal counsel should be sought to determine the need for subpoena or legal process. The data obtained from the MCC HRC survey and from informal interview of committee members determined that most departments do not affirmatively use social media in the investigation by Internal Affairs agents.

[i] ***How Social Media Is Changing Law Enforcement*****,** http://www.govtech.com/, Wayne Hanson, December 2, 2011.

[ii] Memorandum Establishing Social Media Teams, Lieutenant Michael Pavlik, Criminal Intelligence Branch, Criminal Intelligence Operations Division, Metropolitan Police Department, Homeland Security Bureau.

HOW EMPLOYEES SHOULD USE SOCIAL MEDIA

In previous sections of this report social media is shown to be a useful tool for the agency. It is also a popular and much used instrument among employees. Therefore, any policy directing the use of social media should include a section on employee personal use.

Social media is a great way for employees to interact with family, friends and even others in the law enforcement community. However, if not monitored properly, social media can be detrimental to the officer's safety and that of their family and the fellow members of their agency.

As an example, "[i]n October of 2010, Phoenix Police made a DUI stop and discovered a CD with many photographs and names of more than 30 Phoenix police officers and civilian employees that had been culled from Facebook profiles and named as targets." [i] The information published and consequently retrievable through the Internet is generally open to the public if not properly protected. It is especially important that law enforcement employees know how to negotiate and update the privacy settings of each social media account they use.

Not only does the use of social media have the potential to place agency employees in danger, the improper use of social media can lead to disciplinary problems. Any postings by employees, in words or photographs that show the agency in a negative portrayal, can lead to trouble for the employee. In most public behavioral activities, employees of law enforcement agencies are held to a higher standard than the general public. In a survey regarding social media, conducted in 2013 by the Major Cities Human Resources Committee, 63.2% of the 20 agencies surveyed responded that "unprofessional representation of the department to the public" was an employee behavior they were experiencing. However, those agencies making up the nearly two thirds who responded also stated that this unprofessional behavior was less than 2% of their disciplinary actions. Though the number of officers disciplined regarding social media is low, the impact of their postings could have a major effect on the agency's image and credibility. "Nationally, officers have been disciplined and lost jobs over posts on social networking sites. The internet abounds with stories about them." [ii]

Another problem related to postings on social media sites is it can have an impact on an employee's testimony in court proceedings.

> "And defense lawyers increasingly scour social networking sites for evidence that could impeach a police officer's testimony. In one case in New York, a jury dismissed a weapons charge against a defendant after learning that the arresting officer had listed his mood on MySpace as 'devious' and wrote on Facebook that he was

> watching the film 'Training Day' to 'brush up on proper police procedure'." [iii]

POLICY:

Many agencies, including those who participated in our Major Cities Chiefs Human Resources Committee survey, indicate that their agency or municipal government have some type of policy regarding social media. Agencies with a policy that governs the use of e-mail, the Internet and/or mobile data terminals are advised to include specifics when addressing the use of social media. "Such policy direction should include but not be limited to the following:

- Ensuring officers do not indicate their affiliation with the agency when networking
- Prohibiting posting photographs that are taken on department property and/or while in uniform, including official department training, activities or work assignment
- Ensuring that utilization of social networking Web sites, blogs, Twitter or other medium or electronic communication is not done during office-duty time and that any proof that this has occurred on duty and/or on department computers will result in discipline
- Prohibiting posting confidential and sensitive information along with photographs of ongoing criminal or administrative investigations.
- Advising officers that an appropriate level of professionalism should be followed so as not to be detrimental to the mission and the function of the agency.

In a time where the legal standards regarding privacy issues are being interpreted at all levels, the need to ensure clear standards are in place is more important than ever." [iv]

TRAINING:

As with any new or existing policy within the agency, if the employees are not given training in its meaning and application, the chances are not good of it being effective. The training should not focus solely on the bad side of social media but include the positive ways employees can use social media to help the agency and the public they serve.

Given that no one in the agency is immune to the pitfalls of the improper use of social media, this training should start with the chief executives on down.

> "Provide social media training for your officers and staff. Once your policy is written, be sure to distribute it with conversations about departmental support for social media. That would be a good time to roll out training in the various tools. Social media tools scare

> some people. They shouldn't. However, scary things can happen if they are not understood, a little knowledge goes a long way.
>
> While a social media policy is essential for any law enforcement agency, whether it has its own online presence or not, the creation and communication of the policy is perhaps the most important factor in online activity." [v]

NOTE:
It's important to note that employees, regardless of rank or classification, engaging in social networking must strictly adhere to any and all existing federal, state and local laws; policies of the City/County and Police Department; and laws regarding public information on arrests, investigations, and personnel data and resources (i.e. FMLA, ADA, EAP, Behavioral Science Unit (BSU)).

[i] A survival guide for cops on Facebook – Stevens, PoliceOne.com, http://www.policeone.com/pc_print.asp?vid=3298575 retrieved from the internet 1/29/13.

[ii] PilotOnline.com, Police officers urged to use caution with social media – Wilson, http://hamtonroads.com/2011/06 from the internet 3-12-13.

[iii] The New York Times, Police Lesson: Social Network Tools Have Two Edges – Goode http://www.nytimes.com/2011/04/07, from the internet 3-12-13.

[iv] Eric P. Daigle, "Chief's Counsel: Social Networking Policies: Just Another Policy?" The Police Chief 77 (May 2010): 80-82 http://policechiefmagazine.org from the internet 3-12-13.

[v] ConnectedCOPS.net, The Ingredients of a Solid Social Media Policy for Law Enforcement Agencies – Stevens, http://connectedcops.net/2009/08/17. from the internet 3-12-13.

MALICIOUS USE AND SECURITY ISSUES

Suggestions for Social Media Director

Law enforcement agencies who utilize social media would be wise to adjust their security protocols for their official governmental pages, to those suggested by major social media websites such as Twitter and Facebook.

How To - Report a Twitter Impersonator

Unfortunately, there are some individuals who, for either malicious or other reasons, set up impersonating accounts that can confuse the public who are seeking reliable information from your agency. Impersonation is against the Twitter Terms of Service and may result in suspension of the offending account. While Twitter is unable to review the millions of accounts that currently exist, they have set up a system where an agency can easily report abuse of the Twitter Terms of Service. Additionally, it is not necessary to be the owner of the Twitter account to report impersonation.

To report an impersonating account an agency needs to navigate to Twitter link: https://support.twitter.com/forms/impersonation. The form should be filled out completely and clearly as to how the reported account is impersonating your agency online. It may be helpful to link to specific tweets that the account posted. If assistance is needed to find a link to a tweet, you may use this article from Twitter.

Adjust Your Facebook Profile Privacy Settings

IACP advises us on their website about malicious use of social media and how to take precautions with your settings:

> Facebook also allows users to customize their individual privacy settings. Users can control the amount of information they share and which people and applications have access to this information. It is important to take precautions to protect the agency online and having strong privacy settings is one way to do so. Because Facebook often changes the options and default settings, it is important to your agency to check the privacy section frequently. It is also important to remember that there is always the possibility that something posted on the Internet can be shared beyond how it was intended. Therefore caution is recommended on what content is posted on social media sites.[i]

Social Media: A Balancing Act to Benefit Law Enforcement Agencies

While Mitigating Negative Aspects

The use of social media by a law enforcement agency provides positives and negatives to both the agency and to the citizens they serve. It provides access for each to the other, and streamlines rapid communication. We also know social media is a growth industry and the end of its use does not appear to be soon. As a result, law enforcement agencies must carefully plan and monitor the use of these tools to benefit the agency and the community. However, there is destructive potential and police must be vigilant in monitoring for negative outcomes as a result social media.

The benefits of using social media are arguably critical to the mission of pubic safety agencies. Police agencies disseminate information to large numbers of people who can serve as the eyes and ears on the street to help investigators. Through social media, police agencies also push out information that clarifies misconceptions regarding Police actions in order to garner support from the community and to receive feedback and a gauge on how their actions are viewed in the community. The survey conducted by the MCC HR committee found that in the last two years the majority (95%) of the agencies that responded had less than 2% of employees with disciplinary actions due to inappropriate use of social media. One would contemplate that this statistic suggests that many fears regarding the use of social media are unwarranted.

However, use of social media can result in negative outcomes that must be dealt with. One negative outcome is that social media has the potential to become volatile. Volatile instances have occurred when followings of emotionally charged issues on social media gather momentum. In volatile instances, people may add their own commentary, and others may modify it by adding, opinions, photos and videos. The interaction has the probability of becoming dynamic, and may result in impassioned interaction. Law enforcement agencies are an attraction to those types of issues on social media, and depending on the issue and the constituency, the agency involvement may become a source or stimulus for the energy that is created in social media environments. Some examples of social media with negative outcomes include flash mobs, and viral videos. [ii] In addition, since social media can produce immediate response, many use it to vent. [iii]

Another potential negative aspect of social media is the posting of photos and videos. Obviously, pictures and videos taken by citizens can assist police agencies in solving crimes. However, the pictures, videos, and information released by citizens through social media can also compromise officer safety. For instance, broadcasting the location of officers approaching a house in a hostage situation may alert the hostage taker and endanger the hostages and hinder the efforts of the officers. Similarly, someone who is viewing an arrest situation and Tweeting every action of the arresting officers, may divulge critical or confidential information regarding tactical operations.

Social media may also make officers more vulnerable to personal attacks. Detractors of officers doing their jobs well, criticize and attempt to impugn their character. The information reported on social media does not need to be true, but any questions regarding officer character can become an issue in court proceedings. As pubic records become more easily accessed, officers' personal information may be exposed to the public through social media. This potential access makes officers and their families more vulnerable and places them at greater risk. [iv]

In the last decade, much attention has focused on the issue of the right to videotape. In recent years, some courts have ruled that videotaping police in a public setting is a First Amendment right. Two of these cases are referred to for illustration. In 2010 Anthony Graber was charged with violating wiretap laws and threatened with 16 years in prison for videotaping his traffic stop in Maryland. The judge dismissed the charges. In 2011, Simon Glik (Glik v. Cunniffe) was arrested for making a cell phone video of an arrest in Boston. The court held that he was exercising his first amendment rights and received $170,000 in damages and legal fees. [v]

Another case united two disparate allies, the ACLU and law enforcement. Illinois is a two party consent state regarding recording of conversations and events, both audio and visual. That means all parties must agree to the recording of any event or conversation. Since the police did not agree to the recordings, the ACLU launched a pre-emptive lawsuit to block enforcement of the wiretap law. Originally a federal district judge ruled against the ACLU but the court of appeals reversed and ordered a trial. The appellate court held that the statute unconstitutionally limited free speech. [vi]

Some citizen videotapes have been used to demonstrate improper actions on the part of law enforcement, many times for excessive use of force. One website informs the public on how to videotape police actions and stay within the law. [vii] Some citizens have attempted to use videotape for cop baiting. These perpetrators try to provoke a situation that may lead to a fight with officers and risk a citation or arrest in hopes of proving they were treated badly. Their scheme is to facilitate a payout through filing a financially rewarding lawsuit. [viii] In these situations officers must rely on their training and not rise to the bait. They must carry out their duties as they would if no one was taping and let the tape show them following established policy and procedure.

Social media is an opportunity for police officers at all levels, and all should sufficiently train in using social media in order to feel comfortable using it in their efforts of community policing and problem oriented policing. Once they are sufficiently trained, they may use social media to discuss what officers are doing and explain why they are doing so. This helps citizens to understand and improve police and community relations. Social media then becomes a tool for openness and transparency. Officers need to be routinely trained to better understand how social media should be used and for continuous improvement of their job skills. Law enforcement officers need to be reminded what they should and should not say and do when they are using social media. Training must focus on what is appropriate and should be provided on all aspects of social media. The survey conducted by the MCC HR Committee found that less than half (42%) of the responding agencies provide training on social media. As in all aspects of their job, it is important to ensure officers understand that they have a different standard to live by, and they must set an example as community leaders. Discretion is needed regarding what is said by law enforcement officials on social media sites. But when mistakes are made regarding what is posted, these mistakes should be corrected supportively, with remediation in mind, not punishment. Those that repeat irresponsible acts must discontinue their use of agency related social media. [ix]

According to our MCC survey, 84% of the responding agencies considered the use of social media by employees on and off duty to be a concern. To protect employees, law enforcement agencies should put mechanisms in place to minimize the various threats from social media use. One of those mechanisms is for agencies to implement a comprehensive social media policy. The survey also found that most agencies (95%) have some type of social media policy. Where appropriate, agencies should designate a social media manager to provide the on-going training for employees. The training should include instruction to eliminate personal information from individual social media. The manager's job may also include providing agency alerts to potentially negative posts. Monitoring commentary about the department and its personnel is essential. Optimally, the manager can capitalize on agency strengths, but identify and mitigate negative images and potential danger. This includes identifying risks, then preparing and implementing strategies of defense. Part of the manager's job should be to monitor websites and provide an early warning system against threats, while similarly, monitoring trends and incidents. This includes being on the lookout for criminal events that foster copycat behavior. High priority should be on promoting unceasing awareness, providing leadership through social media education, training, and to diligently manage employees on-line exposure.[x]

In the comments section of the MCC HR Committee survey, two concerns were predominately identified. The first was the expectation of the public for quick turnaround of information and the burden on agencies to continually update and provide that information. The second was the regret of posting something too quickly and dealing with the fact that once something is out it cannot be taken back. These are important issues but with proper leadership they can be mitigated. From the MCC HR Committee research and subsequent product on the social media project, two recommended policies become evident. The agency needs to staff the social media initiative, and second, there is a strong need for commitment from command staff to provide sufficient training.

As mentioned previously in this study, Police Chief Magazine published nine steps for success in implementing social media in policing. These steps are appropriate for a summary and conclusion of this study.

1. Have a Strategy
2. Create a Department Policy
3. Assign Staff
4. Technology is Not the Answer
5. Abandon Fear
6. Do Not Abandon the Effort
7. Avoid Anonymity
8. Twitter is Two-Way
9. Get Help if You Need It [xi]

Social media can and should be used as a tool to help law enforcement agencies fulfill their mission.

[i] www.iacpsocialmedia.org/Resources/ToolsTutorials/ViewTutorial.aspx?cmsid=5941&termid=128&depth=

[ii] Social Media and Law Enforcement, Potential Risks, Gwendolyn Waters, FBI Law Enforcement Bulletin, November 2012

[iii] .Social Media Beat, Mark Economou, IACP Center for Social Media, http://blog.iacpsocialmedia.org

[iv] Social Media and Law Enforcement, Potential Risks, Gwendolyn Waters, FBI Law Enforcement Bulletin, November 2012

[v] Courts Side with ACLU on Videotaping Police, Law Enforcement and the Law, Ken Wallentine, June 11, 2012, PoliceOne,com

[vi] A New First Amendment Right: Videotaping Police, Adam Cohen, May 21, 2012, http://ideas.time.com.

[vii] 7 Rules for Recording Police, Gizmodo, Steve Silverman, April 10, 2012

[viii] Social Media and Law Enforcement, Potential Risks, Gwendolyn Waters, FBI Law Enforcement Bulletin, November 2012.

[ix] Police Officers Warned to Treat Tweeters With Care, Sandra Laville, the Guardian, October 2, 2012 , www.guardian.co.uk; Police Chief.

[x] Social Media and Law Enforcement, Potential Risks, Gwendolyn Waters, FBI Law Enforcement Bulletin, November 2012

[xi] Police Chief, January 2013, Social Media in Policing: Nine Steps for Success, Lauri Stevens, www.policechiefmagazine.org

Social Media: A Means to Inform, Educate & Gauge Public Interest in Law Enforcement Issues

In the decade since its inception, social media, such as Twitter, Facebook, YouTube, etc., has become a powerful tool for communication. As of late 2011, three-quarters of American adults use the Internet, and of those, nearly 80% visit social media sites or blogs, meaning two-thirds of Americans are using some form of social media[i]. The proliferation of social media and mobile phones over the last decade has spurred significant interest in their use in various segments of the private sector particularly in the business, education, political and civic communities. Today, these new communication tools are actively being used by traditional civic and political stakeholders to foster community initiatives and electoral campaigns.[ii] Increasingly, the general public turns to the use of these new technologies as providing an opportunity to encounter public affairs news and discourse, enhance understanding of issues, and get involved in civic and political activities. Moreover, social and mobile media platforms have created new channels and means for citizens to interact with governments and other political institutions, monitor their functioning, and more actively participate in policy-making processes. There is little doubt that the emerging social and mobile media practices are changing the public's understanding of governance and politics.[iii]

This is especially true in the area of law enforcement where the development and implementation of community policing provides an already existing platform for the general public to engage their government. It is well settled that the key component of the community policing strategy focuses on building strong partnerships with the community by creating an environment in which community members are comfortable sharing information with law enforcement and keeping the lines of communication open between citizens and their local law enforcement agencies. The growing use of social media by law enforcement agencies represents an innovative way for the police to continue to strengthen ties with various segments of the community and the next logical step in the manner law enforcement interacts with the community at large.

Social media has become a powerful tool for law enforcement in its attempts to reach a broad swath of the community. According to a recent survey of more than 1200 *Federal, State, and Local Law Enforcement Professionals,* 83% of current users anticipate using social media more, while 74% of those not currently using it indicated they intend to start using it. [iv]

The proliferation of the use of Facebook and Twitter by law enforcement clearly demonstrates that law enforcement agencies are using social media to communicate and interact with the community. It is less clear to what extent police departments are managing these tools and what problems or barriers public agencies are encountering with social media. We don't yet know how well we are managing the expectations of the community that now have a direct route to communicate with law enforcement on a 24 hour basis. This section will explore the use of Social Media tools to inform, educate and engage the public on law enforcement issues.

Social Media: Communication Changes

As stated above, government agencies, including law enforcement, have enjoyed tremendous success in the use of social media tools to inform and educate the public. Originally created to connect people with other people, Twitter and Facebook have evolved into a major method law enforcement and other public sector organizations connect with consumers and constituents. Prior to social media, police departments would communicate with the public through newspaper notices, public postings, radio and television commercials, direct mailings, or other traditional methods. Agencies had little way of knowing if the information was being read or how the community reacted to it. Given the expense of traditional media, communication was necessarily limited. Social Media tools allow public agencies to communicate more frequently and more directly in nearly real time with constituents at little or no cost. According to the 2010 survey of the International Association of the Chief of Police (IACP) 40 percent of agencies in the U.S. are already using platforms like Facebook, Twitter, YouTube and similar media to solicit tips. Most others -- 80 percent according to the IACP survey -- use social media in some capacity. [v] While it appears that law enforcement has concentrated on using social media to solicit the public's assistance to help solve crimes, there is strong evidence that the most beneficial use of social media tools is one that has the least negative impact on law enforcement. It is the use of these tools to inform the public of emergencies, to educate the public on law enforcement issues, and to celebrate the victories in law enforcement with the general community.[vi]

A. One Way Communication: To Educate and Inform

From wanted posters used in the early growth of American society, to the police radio made popular during the Industrial Revolution, and then to patrol cars, the need of law enforcement to communicate with the public has always existed. Today, the communication tool of choice is the use of social media. Because social media channels offer such an amazing way to spread information, it's natural that many web services exist to keep citizens informed of important issues. CrimeWeb is a free, centralized, web-based clearinghouse for public safety information that is currently being used by many local government organizations across the US. Users can sign up to get alerts about missing children (Amber Alerts) and adults (Silver Alert), homeland security updates, major crimes and fugitives, as well as local community information. Similarly, crime data mapping web site SpotCrime offers free crime alerts by email, and also sells crime tracking iPhone applications (iTunes links) for New York City, San Francisco, Chicago, Baltimore, and London. Increasingly, law enforcement agencies have enjoyed great success in using social media to alert constituents about evolving emergency situations, increasing public knowledge about agency policies and goals and soliciting feedback on issues or initiatives being considered by the agency.[vii]

Mainstream social networking tools are also being used to keep the public informed and connected. The use of Twitter and Facebook to post information has increased substantially in law enforcement. The appeal of Twitter and Facebook to the law enforcement community is the immediate response an agency can get by monitoring the number of "Likes" or Comments it gets when posting information. Moreover by using social media, police departments are able to communicate with constituent groups that have expressed an interest in receiving information from the agency.

The Dallas PD, for example, uses Twitter to put out crime alerts, as do the police in Boston, the District of Columbia, Fort Worth, Houston, and Philadelphia. The Police Departments in the District of Columbia and Philadelphia use both Facebook and Twitter to connect with the public and answer questions.[viii] And in smaller jurisdictions, like the newly created town of Dunwoody, Georgia, the local police use social media to build community ties and introduce the department to its new neighbors.[ix] While Twitter and Facebook seem to be the recognized utilization of social media, there is a trend for law enforcement agencies to use other types of social networking tools to educate and inform. Several Major Cities Agencies currently use their public webpages to post redacted police reports. Police Departments in the cities of Philadelphia, Seattle, and Washington, DC, also post redacted police reports to raise the awareness of the public about crimes in particular neighborhoods, or trends in criminal activity.[x] Seattle and Philadelphia report wide success using this tool to inform the public.[xi]

B. Two Way Communication: To Build Partnerships & Improve Police/Community Relations

Another social networking tool that is experiencing some success is the use of list serves and other forms of social media tools to communicate with particular communities. These tools allow for the cross-communication of issues between various communities. When law enforcement agencies use Facebook and Twitter to inform the public of events and issues of concerns, the degree to which there is two-way communications may be limited. The agencies issue the information and the citizenry can choose whether or not to act on the information, and there is no requirement that individuals in the community interact with the law enforcement agency. However, when agencies move from the well known Twitter and Facebook to social networking tools such as community list serves, like Tweet-Along, there is an expectation that the communication is two-way. In fact, those law enforcement agencies that have set up list serve and other types of email do so with the primary intention of engaging the community to foster more meaningful relationships with the citizens they serve. One example is the

Arlington, Texas, Police Department that has experienced great success in its Tweet Along Program. Citizens who had been on a ride-along tweeted their experience to the Arlington PD Website. Arlington re-tweeted these accounts to various groups. The response they received from the citizens of Arlington, as well as citizens and police departments across the nation, was tremendous:

> Other departments around the nation also followed us and gave us a great sense of connection not only to the citizens following and participating, but also to our colleagues in law enforcement in other cities. This event is great for providing the experience to anyone who could not participate in a real ride along with an officer. It gives a greater number of persons the experience, without as many safety concerns to either the citizen or the officer. [xii]

The DC Police Department uses its civilian community outreach coordinators to establish community list serve in all seven police districts. Some districts have created several list serves depending on what issues the list serve is intended to address. The communication not only flows between the MPD and the list serve participants. When necessary, MPD may function as a facilitator in "hosting" a community chat between various community groups where there are issues of common concern. The online email discussion groups have been in existence since 2004.[xiii] According to its webpage, the online discussion group was created specifically to bring various community groups together:

> The MPD police community discussion groups were created in 2004 for members of the community so they could share public safety information in an effort to help reduce crime and the fear of crime. Information shared on the online email lists includes public safety community announcements and meeting dates; crime statistics; safety concerns and ideas; crime reports; and safety tips. The online email list also acts as a virtual community, which helps strengthen partnerships between the local police and the communities they serve. It also offers another means of visibility and accessibility for the community.
>
> The online email list discussion groups are designed to attract area residents, employees, students, business owners, elected officials, and government agency representatives interested in coming together to solve problems and share public safety-related information that will improve the quality of life in each police district. This is an opportunity for all stakeholders and DC service providers (i.e., DPW, DCRA, etc.) to engage in ongoing online interaction with police, 24 hours a day, 7 days a week, holidays and weekends. Information posted to the groups is intended to benefit members of a specific police district.[xiv]

The police departments in Philadelphia and Houston also have list serves, as do many police departments in the San Francisco area. [xv] It is clear that the list serve concept can be a great two-way communication tool for law enforcement to build and strengthen partnerships with the diverse communities that exist in every law enforcement jurisdiction. According to the President of IACP, "engaging citizens through social media including two-way communication, allows law enforcement leadership to humanize their work and their officers, disseminate information, and directly engage with citizens through the online communities in which they participate." [xvi] "Social media's biggest benefit [for law enforcement] has been the daily interaction between the department and the citizens. It has allowed the department to provide more of a personal approach to its services," said Lynn Hightower, communications director of the Boise, Idaho, Police Department (BPD).[xvii]

Two-way communication between the law enforcement community and the citizens they serve does not come without risks. Police departments who use list serves and other email groups, report that agencies have to continually reiterate that these methods of communication are not a substitute for 911 emergency calls. This is by far the single most concern raised by law enforcement.[xviii] What is key to managing social media and the expectation that the list serve is a replacement to 911, is in setting out clear rules of engagement to the users of the list serve. Another problem with the two-way communication method is the inability of the agency to control what is placed on the list serves, particularly as it relates to verifying information. For example, people in the community have used law enforcement list serves to post unsubstantiated accusations.

> "Citizens tend to use the site to report crimes or submit information that would need to be vetted. The site should never be used to take the place of 911. The list has also been used to insult others, submit links to business, or report things that MPD knows to be non-factual. When untrue statements or insults are posted we are able to deny these types of postings.[xix]

These issues can be managed by establishing strong policy and procedures, and regular monitoring of the list serve site. This should include immediate deletion of information that is outside the scope of the list serve, and deletion of inappropriate information intended to defame or slander individual members of the community. (Note: There are first amendment concerns if the libelous content is aimed at the police department or individual members of the police department. Agencies should check with their general counsel before deleting information from its public websites that have been sent in by citizens.)

Notwithstanding these issues, arguably, the benefits of two-way communication outweigh the risks. List serves have increased the visibility, support, and good will of local law enforcement in ways that traditional methods of communicating with the public cannot.

C. Managing Expectations of the Public: Establishing Strong Social Media Policies

If law enforcement agencies want to enhance the partnerships they create within their communities, all departments large or small must recognize that social media have infiltrated modern culture and impacted the workplace. Departments that have embraced social networking recognize that this new platform allows them to connect with citizens on a 24-hour basis. These departments also realize that if they engage in the use of social media tools without thinking through how this tool is to be integrated into the overall work of the department; the very tool that brings police departments closer to its stakeholders can also be divisive. What steps, if any, must a department do to ensure that their use of social media will work to their benefit?

The answer is not a new innovative tool. The answer is research, planning and strategic leading. That includes planning its use, how it is to be introduced, holding people accountable for monitoring, and the planned responses for unintended consequences of the public having direct access to the department almost without filtration. The IACP has published the following nine steps a department must take in order to establish a social media policy.

1. Have a Strategy;
2. Create a Department Policy;
3. Assign Staff;
4. Technology is Not the Answer;
5. Abandon Fear;
6. Do Not Abandon the Effort;
7. Avoid Anonymity;
8. Twitter is Two-Way; and
9. Get Help if You Need it.[xx]

Even before agencies get to the step of establishing the policy, there are key issues the agency must address before placing the department on the social networking train. Citizens expect directness, feedback, and honesty.

> People posting comments on social media sites are as influential as having a face-to-face conversation with someone we know.
> Mass social commentary through websites can define issues. Mass commentary via social media can dominate mainstream media. [xxi]

To law enforcement this means that the information used must be truthful, interesting and serve a purpose for the stakeholders who access the site. To this end, before establishing a social media page intended for one or two-way communication, agencies should review their policies and determine which ones will be effective in a social media setting. Second, agencies should evaluate their websites to ensure that it is user friendly, interactive, accessible and attractive. The law enforcement agency may have the internal expertise, or they may need to consider hiring a professional to establish the website.

The use of social media will create a public image of the agency. The information placed on the website may have a positive or negative impact on the agency's standing in the community. As such, agencies should create the "personality" they want to convey to the public and ensure that all social networking tools convey the same personality or image. In order to do this an agency must review the policies and documents it will use and determine whether these convey the same message no matter how the information is disseminated online. Additionally, the information needs to be user friendly. In other words, the agency needs to be approachable and responsive.

As mentioned before, agency websites need to be strategically planned. If the purpose of the website is for citizens to seek out the agency and obtain information about its activities, then the content posted must be relevant, truthful and responsive. To do this the agency must make certain that the customer experience is integrated into all information provided on the site. Part of that information may include telling the stories of successes and acknowledging failures. To the extent possible, the goal should be connecting people to their information of interest, and helping the agency build relationships with its community. To do this, individuals should be offered a friendly non-bureaucratic experience, aimed at creating a meaningful dialog with them. For success in these endeavors, the agency must research and test whether visitors to the website can find quick answers to their questions? That research will determine whether the agency is fully engaged and effective in communicating with their communities.

These may be new issues for law enforcement bureaucracies to address. However, success requires the agency to engage in these types of considerations before embarking on social media networking in the community. As mentioned above, an area of importance is the identification the information most sought by the community being available online. Arguably, making information available in this way will cut down on traffic in the agency headquarters and frees staff to concentrate on other areas. Below is a list of links on the DC MPD website where MPD lists all the different public documents citizens can access without having to come into MPD's buildings. These include certain general orders, online police reporting, crime analysis and mapping information, and a variety of other topics: Each topic has an interactive link that enables the citizen to access information and to relay and upload information:

MPDC Popular Links

- MPD Services
- Careers with MPD
- Find my Police Service Area & Police Commander
- Register a Firearm
- File a Police Report Online
- Contact the Police
- File a Complaint or Commendation
- Police Telephone / Contact Directory
- Volunteer Programs & Internships with MPD
- Contest a Ticket
- Locate a Towed Vehicle
- Media Info [xxii]

Philadelphia, Seattle and Houston PDs use their websites similarly.[xxiii] In fact, the use of various social media tools by the Philadelphia PD has been recognized nationally and internationally:

> The Philadelphia Police Department is enjoying great success using social media. According to IACP, we have the most popular Facebook page of any municipal law enforcement agency in the United States. Our efforts have been profiled by many publications such as NPR, ABC National News, GovernmentTech magazine and many more.[xxiv]

The use of social networking tools has proven to be a powerful ally to law enforcement to further strengthen and develop community partnerships. These tools enhance agencies' abilities to fully engage the communities they serve and create an atmosphere of transparency and openness. Agencies can increase their capacity to use social media tools in community policing by carefully examining the agency goals and establishing social media policies that will aid agencies in accomplishing these goals. If done correctly, agencies can use social media tools to tout successes and build strong community partnerships that ultimately lead to establishing safe communities' throughout the country.

Social Media: A Means to Develop Partnerships Between Law Enforcement and the Community

As a starting point and context, it took radio 38 years to reach 50 million listeners. Terrestrial TV took 13 years to reach 50 million viewers. The Internet took four years to reach 50 million users. **In less than nine months, Facebook added 100 million users.**

The single most important crime-fighting tool for law enforcement has been assistance from the public. This can be in the form of a witness at a crime scene, or a person calling their local precinct, or the anonymous crime stopper hotline that has been used with tremendous success for decades. This methodology has served law enforcement well for years. Technology and generational differences in the way younger people are communicating are changing the way to conduct business.

As the economic cycle comes and goes, law enforcement departments all over the country are required to do more work policing with fewer personnel. Departments are relying on technology to assist them in crime prevention and in crime fighting. Agencies are combining their community policing efforts with intelligence led policing, and then morphing into predictive analyses. Utilizing social media is a critical part of these efforts.

Departments can use social media tools to enhance community policing initiatives by promoting better communications, providing greater access to information, fostering greater transparency, allowing for greater accountability, encouraging broader participation, and providing a vehicle for collaborative problem solving. For example, crime prevention tips may be posted through various online avenues, online reporting opportunities may be offered, crime maps and other data may be posted, or these tools may be used to distribute valuable community and alert information.

Texting to Law Enforcement Example

Why's It Becoming So Popular?

There are two main reasons. One from the law enforcement side, the other from the tipster's point of view. First, cell phones are everywhere, from the highways to shopping malls to your living room. Practically everyone has one, so tips can be sent almost at the same time as the tipster sees or hears something suspicious. This is a great advantage to the police.

The second and perhaps most important reason is that the police go to great lengths to make sure that tipsters know that their texts

> are absolutely anonymous. And that makes sense. It seems like law enforcement agencies have been stymied by the public's "no snitching" rules forever.
>
> Witnesses are afraid to come forward with information about crimes out of fear of retaliation by the suspect or his friends and cohorts. If the system wasn't anonymous, people wouldn't use it; it simply wouldn't work.[xxv]

[i] Nielsen. (2011). State of the Media: The Social Media Report Q3 2011. Nielsen. Retrieved from http://blog.nielsen.com/nielsenwire/social.

[ii] BLOG: http://inesmergel.wordpress.com/ **Social Media in the Public Sector: Social Networks,-Social Software-Social Technologies, February 27, 2013** citing: *"Call for Papers: Transformation of Citizenship and Governance in Asia: The Challenges of Social and Mobile Media", January 11, 2013; Journal of Democracy and Open Government,*

[iii] Id

[iv] Sponsored by LexisNexis, The research conducted in March 2012 assessed the law enforcement community's understanding of, proclivity to use, and actual use of social media, and aimed to better understand acceptability thresholds of various types of investigative techniques and current resources and processes being used. The nationwide survey was conducted online and solicited feedback from more than 1,200 participants at every level of law enforcement – from rural localities to major metropolitan cities to federal agencies – producing a comprehensive view of the social media landscape. Respondents are active law enforcement professionals ranging in age, experience, and job level.

[v] "Social Media Elevates Community Policing", by Indrajit Basu; August 12, 2012 , Digital Communities, http://www.digitalcommunities.com/articles/,

[vi] **Social Media Use In Local Public Agencies: A Study Of California's Cities**, Christopher Gerard Zimmer, Department of Public Policy and Administration, California State University, Sacrament, Spring 2012 citing Facebook. (2010***). "Connecting with your Constituents with Facebook".*** Facebook. Retrieved from
https://facebook-inc.box.com/shared/idnp0hs026..

[vii] Id

[viii]*" **Virtual Neighborhood Watch: How Social Media is Making Cities Safer",*** **http://mashable.com/2009/10/01/social-media-public-safety/,** Josh Catone, October 2009

[ix] *"**How Social Media Is Changing Law Enforcement",*** Wayne Harrison, Government Technology: Solutions for State and Local Governments, December 11,2011; http://www.govtech.com/public-safety/How-Social-Media-Is-Changing-Law-Enforcement.html?page=4

[x] *"**How Social Media Is Changing Law Enforcement",*** Wayne Harrison, Government Technology: Solutions for State and Local Governments, December 11,2011; http://www.govtech.com/public-safety/How-Social-Media-Is-Changing-Law-Enforcement.html?page=4

[xi] ID

[xii] Major City Chiefs Human Resources Committee 2013 Survey on Social Networking in Law Enforcement, Question 14.

[xiii] MPD, Online Discussion Group, http://mpdc.dc.gov/node/207402.

[xiv] Id.

[xv] Id. at footnotes 10 and 12.

[xvi]

[xvii] "*Social Media Elevates Community Policing*", by Indrajit Basu; August 6, 2012 , Digital Communities, http://www.digitalcommunities.com/articles/,

[*xviii*] Id.

[xix] Comment, Ms. Fayette Vaughn-Lee, Acting Director, Community Outreach Division, DC Metropolitan Police Department; in response to question 4, Social Media Survey, HRC Committee, Major City Chiefs Association, February 22, 2013.

[xx] Social Media in Policing: Nine Steps for Success, Lauri Stevens, Police Chief Magazine, http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display&article_id=2018&issue_id=22010, retrieved from the Internet 5/27/13.

[xxi] ***"Government and Social Media--Creating Meaningful Experiences",*** By Leonard A. Sipes, Jr., Senior Public Affairs Specialist/Social Media Manager Court Services and Offender Supervision Agency, http://www.corrections.com/links; 1/31/2011

[xxii] DC MPD Home Page; http://mpdc.dc.gov/

[xxiii] MCC Survey, Id at footnote 14.

[xxiv] Id

[xxv] *Lawyers.* March 7, 2013. <http://criminal.lawyers.com/Criminal-Law-Basics/Text-Messaging-or-Texting-Crime-Tips.html>

What is Twitter?

Twitter is a micro-blogging tool that allows users to send short messages (140 characters or less) that will immediately be distributed to their network of followers.

How can law enforcement use Twitter?

Twitter allows law enforcement agencies to send out immediate updates to large groups of people anytime and anywhere. Twitter can be used to distribute traffic alerts, disaster preparedness and response information, news, prevention tips, and event details. Users can also use this service to link to their existing website, press releases, or other information.

Becoming Your Own News Station: YouTube and Facebook

How can law enforcement use YouTube?

YouTube allows an agency to be its own news station by establishing a place to post video about the topics and events it deems important. This service also allows community members to watch videos at their convenience.

Crime Solvers Information — Agencies can post surveillance video in conjunction with tip line information on YouTube, giving a large audience the opportunity to provide crucial suspect and crime information. Soliciting help on solving crimes also helps police departments tell the community what is going on in their area.

Recruitment — Agencies can post videos that highlight academy graduations or that are recruitment-specific, showing what it takes to be an officer in your agency. These videos will give unique insight to potential recruits that they may not receive from a flyer or a visit to the agency web site.

Crime Prevention and Safety Tips — Videos can be an effective way to share crime prevention and safety tips with the community. The immediacy of YouTube uploading and sharing allows agencies to respond quickly to current issues and to inform the public with little delay. Now the agency can provide video to its community instead of just telling them about safety and crime prevention tips.

Chief's Message — Like a president giving a State of the Union address, an agency's chief and other executive officers can make a video message to the community and use YouTube to share it. Whether it is a monthly video on key issues and events affecting the community or a biannual presentation highlighting the efforts of the agency, a video message from the department shows the community the face of its law enforcement agency and this enhances community relations.

Press Conferences — Often, after a press conference, the public will only receive sound bites that are provided to them by the news media. By capturing the entire conversation and uploading it to the agency YouTube site, the department can give the public the whole story.

Event Promotion and Follow-Up — An agency can reach a wide audience and possibly increase participation in its events by providing the community with exciting video insight into upcoming events and activities. The department can also upload video taken during its events, enhancing community relations by showing the agency in action.[i]

Areas Of Concern with Social Media

Police managers have an unprecedented opportunity to push out information about their Departments that the traditional media either will not or cannot cover. However a few very important items need to be kept in mind. If the department is a large agency with a corresponding Public Information Office in either the County Executive, Mayor, or District Attorney's Office, it is strongly suggested that policies and procedures are put in place to ensure that the information disseminated be in harmony with each of the other executive branches of government.

What Happens When the Lights Go Out

On October 26, 2012, Long Island and the Tri-State Area of New York City started to put their Costal Storm Plans into effect. Super storm Sandy was about 96 hours from reaching landfall on the northeast coast of the United States. For years most police departments and offices of emergency management had been using traditional and social media to keep the pubic informed and advised of appropriate precautions and evacuations. On October 29, 2012, at about 1900 hours, Long Island experienced an unprecedented storm surge that flooded many homes, business and critical infrastructure. The storm knocked out power to nearly a million customers, almost half of Long Island's residents.

The result of storm Sandy was a power outage in many governmental agencies that had become accustomed to using computers and social media to inform residents of potential dangers and information. The agencies were then forced to fall back on older and more inefficient methods of communication. Examples of this were Police Officers on external speakers of their radio cars, electronic signs powered by gasoline generators, and flyers and leaflets manually distributed. One of the lessons learned was that secondary methods of communication must be given serious consideration prior to a catastrophic event.

[i] *International Association of Chiefs of Police.* March7,2013. http://www.iacpsocialmedia.org/Portals/1/documents/Fact%20Sheets/YouTube%20Fact%20Sheet.pdf

COMMUNITY PARTNERSHIPS THROUGH SOCIAL MEDIA

An emerging social networking platform provides a means for neighbors to link online. Nextdoor.com and i-Neighbor.com are two sites that provide a way for people sharing a geographic location to connect without necessarily meeting personally. This technology offers an easy to use, non-threatening means of sharing crime information and related safety reminders within a community. The Dallas Police Department actively utilizes Nextdoor and has set a goal of having 90% of its neighborhoods registered. St. Louis PD has recognized the benefit of using the site to strengthen community/police partnerships, particularly as an easy method for getting information such as alerts regarding crime and suspicious activity to residents.[i] The Chesapeake, VA Police Departments experienced an increase in citizen reports of suspicious activity when they have utilized Nextdoor. This platform provides a non-intrusive method for individuals who are not likely to attend community meetings or actively participate in organized groups to become involved with each other and also with their local police department.[ii]

In its March 10, 2013 article on this subject, the Virginian Pilot referenced data provided by Kelsey Grady, Senior Communications Manager, Nextdoor.com about its site:

> "Nextdoor launched nationwide in October 2011, and has launched more than 9,200 neighborhood websites and is in every state. Nextdoor is a free online platform that enables neighbors to create private school networks for their neighborhood. Using Nextdoor, neighbors can communicate with each other to build stronger and safer neighborhoods."[iii]

Social networking and neighborhood interaction statistics in the U.S. indicate:

- ➢ 65% of all online adults use a social networking site
- ➢ 28% of Americans don't know any of their neighbors by name
- ➢ 79% of Americans who use an online neighborhood forum talk with their neighbors in person at least one time each month
- ➢ 2% of people using Facebook are neighbors
- ➢ 93% say it is important for neighbors to look out for one another
- ➢ 67% of homeowners feel safer in their home/neighborhood because they know their neighbor[iv]

It makes sense for police agencies to not only set-up and maintain their own social networking sites but also to utilize other platforms which complement their efforts in expanding the reach of how and where information is disseminated to the public.

[i] “Online networks link neighbors, can help fight crime in St. Louis area,” Kim Bell, stltoday.com, February 23, 2013.

[ii] “Like a Good Neighbor, Start Warning Each Other Who’s There,” Veronica Gonzalez, Virginian Pilot, March 10, 2013.

[iii] Id.

[iv] Id.

REVIEW OF THE IACP CENTER FOR SOCIAL MEDIA SECOND ANNUAL SURVEY

The IACP Center for Social Media, http://www.iacpsocialmedia.org/, offers the findings of its second annual survey on law enforcement's use of social media tools conducted in August of 2012. The most common social media use reported by responding agencies was criminal investigations activity, tabulated at 77.1%. Intelligence activities were tabulated at 61.7%. The entire tabulation covering 12 activity areas, and a "not used" category, is presented by the IACP Center for Social Media. [i] The tabulation makes it clear that law enforcement agencies are utilizing social media tools to conduct investigative and intelligence activities at nearly the same levels they are notifying the public of crime problems, 63.7%, and conducting community outreach and citizen engagement activities, 61.8%.

The IACP Center for Social Media also offers a new resource, cover dated February 2013, *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations.* This guidance offers law enforcement agencies recommendations and cites legal/technical issues to consider when developing policy related to the use of social media tools and social media derived information for criminal intelligence and investigative functions. The project was grant supported by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, in collaboration with the Global Justice Information Sharing Initiative. The *Guidance And Recommendations* resource may be downloaded at http://www.iacpsocialmedia.org/Portals/1/documents/SMInvestigativeGuidance.pdf.[ii]

The terminology applicable to this subject will continue to evolve rapidly with technological innovations and consumer preferences, but some general terms appearing in the guidance and recommendations are relevant for policy discussion and policy development in any law enforcement agency. There are social media sites, social media tools, and social media resources available to the public, the news media, corporate entities, foreign and domestic organizations and governments, and law enforcement. The policy needs of law enforcement appear to focus on verbs describing activities: accessing, viewing, collecting, storing, retaining, and disseminating or using social media information consistent with legal authority and mission requirements. Limitations on the use of information derived from social media sites pursuant to law enforcement investigative and intelligence activities focus on the protection of privacy, civil rights, and civil liberties of individuals and groups. Add to this complicated scenario compliance with applicable local ordinances, state, federal, and tribal laws. Also of particular importance are the First Amendment, the Fourth Amendment, and the 28CFR Part 23 federal regulation regarding criminal intelligence information systems.

Page 9 of the Guidance and Recommendations lists seven key elements of a social media policy which are presented here verbatim from the resource:

- Articulate that the use of social media resources will be consistent with applicable laws, regulations, and other agency policies.
- Define if and when the use of social media sites or tools is authorized (as well as use of information on these sites pursuant to the agency's legal authorities and mission requirements).
- Articulate and define the authorization levels needed to use information from social media sites.
- Specify that information obtained from social media resources will undergo evaluation to determine confidence levels (source reliability and content validity).
- Specify the documentation, storage, and retention requirements related to information obtained from social media resources.
- Identify the reasons and purpose, if any, for off-duty personnel to use social media information in connection with their law enforcement responsibilities, as well as how and when personal equipment may be utilized for an authorized law enforcement purpose.
- Identify dissemination procedures for criminal intelligence and investigative products that contain information obtained from social media sites, including appropriate limitations on the dissemination of personally identifiable information.[iii]

The Guidance and Recommendations provide a powerful, yet simple, explanation of the authorization levels by drawing parallels between traditional law enforcement actions and social media actions in the context of Apparent/Overt, Discrete, and Covert activity. Uniformed patrol on the street is equated with Google(ing) someone, searching Facebook, and searching YouTube. These actions are termed to be Apparent/Overt. Plainclothes officers and detectives are equated with searching and retaining public access pictures, and retaining profile status updates. These actions are termed to be Discrete. Undercover officers and a full investigation are equated with friending, following, setting up a user account to enable direct interaction, and lawful intercepts. These actions are termed to be Covert. In the Social Media technical realm, law enforcement personnel need to understand privacy settings, end-user licensing agreements, and terms-of-service requirements

In the Apparent/Overt Use engagement level there is no interaction between law enforcement personnel and the subject/group. Apparent/Overt Use is based on user profiles/user pages being open to anyone with Internet capabilities who can access and view the user's information. During the Discrete Use engagement level, law enforcement's identity is not overtly apparent and activity is focused on information and criminal intelligence gathering. There is no direct interaction with subjects or groups. During the Covert Use engagement level, law enforcement's identity is explicitly concealed to enable authorized undercover activities for an articulated investigative purpose, with concealment of officer identity deemed to be essential. An example of Covert Use is the creation of an undercover profile to directly interact with an identified criminal subject online.

The documentation of information derived from social media should specify the purpose of the information use, what information was collected (such as photos, status updates, friends), when the information was accessed and/or collected, where the information was accessed (identify the Web site), and how the information was collected (open search, nongovernmental IP address, undercover identity, etc.). Copies of the information obtained from the sites should be documented in the investigative case files. As law enforcement agencies develop and implement social media policies consistent with the guidance and recommendations in this resource, it may be anticipated that law enforcement accreditation processes will audit adherence to the policy and may require periodic training of all involved personnel to keep up with technological innovations and new legal precedents.

The Guidance and Recommendations state that a social media policy should specify whether or not law enforcement personnel may, when carrying out authorized law enforcement duties, use personal equipment, including personal accounts, to access information via social media sites and should further specify the reason(s) and requirements associated with the use of personal equipment for this purpose. If policy allows for the use of personal equipment and personal accounts, the documentation requirements of the preceding paragraph become applicable to include a record of follow-up actions.

The Guidance and Recommendations are included as an electronic attachment to this project report. Appendix A of the resource cites numerous cases and authorities that should prove useful during social media policy development since the effort will need to cut across many functional specializations within any law enforcement agency to include human resources managers, criminal investigators, background investigators, records managers, information technology administrators, computer forensics experts, internal affairs investigators, legal counsel, and public information officers. Appendix B features the Georgia Bureau of Investigation Social Media Policy, dated October 2012, which may serve as a good starting point to facilitate local agency customization to meet the policy development needs of other jurisdictions.

[i] http://www.iacpsocialmedia.org/Resources/Publications/2012SurveyResults.aspx.

[ii] *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations.* Retrieved from the Internet on June 21, 2013, http://www.iacpsocialmedia.org/Portals/1/documents/SMInvestigativeGuidance.pdf

[iii] Id., p. 11.

SUMMARY OF FINDINGS FROM 2013 MCC HR SOCIAL MEDIA SURVEY

Nineteen responses were received through Survey Monkey and one response was received through email. One agency submitted two responses and one response was anonymous. Where possible, the data provided below is compiled from the Survey Monkey summary report and the information provided separately.

Policy

Half of the twenty responding agencies (50%) reported that their City/County provided the overarching policy for the organization and the department has a companion policy. Other responses included not having a policy, having a policy limited to the department, being in the process of developing a policy and adopting the IACP model policy.

Half of the agencies (50%) reported that their policy focuses on prohibited actions as well as using social media to enhance effective communication and community relations.

Fifteen of the responding agencies (75%) reported that their policy scope included social media usage in addition to internet/email usage.

Most Common Social Media Uses

Most agencies use Facebook for recruiting (15/20 or 75%), community outreach and information (program and events) (17/20 or 85%) and for public safety information dissemination (16/20 or 80%).

Most agencies use Twitter for public safety information dissemination (16/20 or 80%).

To a lesser extent, YouTube is used for community outreach and information and for public safety information dissemination (11/20 or 55%).

Less than half of responding agencies utilize a text alert system for public safety information dissemination (9/20 or 45%).

Only six of the twenty responses (30%) indicate that they utilize smart phone and tablet applications.

Training

Less than half (9/20 or 45%) provide social media training to their employees. Of note, Houston and Raleigh provide a 4-hour block of in-service training. Philadelphia provides an 8-hour training for department members who have authorization to provide Twitter updates.

Employee Use of Social Media

Most agencies (16/20 or 80%) are concerned about employee use of social media on and off duty, but of those who report social media-related disciplinary actions, the volume of disciplinary actions is less than 2%. The predominant behavioral problem associated with social media-related disciplinary problems is “unprofessional representation of the department to the public.”

Response to Citizens

Responses to citizens through social media vary from within the hour to during regular Monday through Friday business hours only. In most cases, the responsibility falls upon the Public Information or Media Relations Officer.

Social Media Successes Reported by Respondents

Social Media:

Provides a means of promoting positive public relations through sharing stories that the media would not share and/or telling the story from the police perspective.

Creates a sense of departmental transparency and facilitates a better partnership with the community.

Gives voice to citizens who support law enforcement agencies by providing citizens with a means of sharing their positive interactions with police officers. Houston set up an employee recognition tool called “Officers in Action”.

Enhances the dissemination of information in a variety of ways (posting videos of crime suspects/Most Wanted or missing persons, promoting programs/events, and broadening scope of recruiting). Also accelerates the dissemination of emergency information regarding natural disasters (often ahead of the media’s response).

Provides a forum for the public to experience virtual policing. Fort Worth’s “tweet-along” with Arlington was well received by the community as a kind of virtual ride-along. Salt Lake City also had a “tweet-along” to promote awareness of holiday DUI situations.

Social Media Concerns Reported by Respondents

Social Media problems are:

Finding best fit for Public Information/Media Relations Officer assigned to social media and providing adequate staff coverage. (Posts must be monitored and vetted carefully yet many agencies do not have staff for 24 hour/day, 7 day/week coverage. Some agencies save screenshots of all deleted posts.)

Confusion between 9-1-1 and social media.

Inappropriate posts (insults, using site to promote private business, etc.).

Employee judgment in posting images in uniform, with department vehicles, etc.

Premature/inappropriate release of information of crime information or failure to coordinate with Public Information/Media Relations Officer.

Funding issues that prevent purchasing mobile applications.

Release of inaccurate information.

Increasing citizen concern or fear by reporting active calls through social media.

Difficulties keeping pace with increased expectations from the public.

Trends

The MCC HR survey listed the following additional Social Media useage:

Instigram and Pinterest (Houston)

See, Click, Fix (Raleigh)

Tweet-alongs (Fort Worth and Salt Lake City)

Use of social media dashboards (TweetDeck, Twittus, Hootsuite, Sprout Social, Radian 6, etc.)

MAJOR CITIES CHIEFS' ASSOCIATION – HUMAN RESOURCES COMMITTEE – SOCIAL MEDIA PROJECT – POLICY REVIEW

April 8, 2013

Fairfax County - Social Media Content Policy

A. SOP Includes in part:

a. Preamble identifying focus of the policy. The policy addresses three areas, official county-maintained Social Media sites, employee access to Social Media while working and employee participation in Social Media while off duty.

b. When discussing official county social media sites, the policy professes a desire to become more transparent, deliver public information to citizens, engage citizens and provide enhanced customer service through electronic means. This section covers Facebook, Twitter, etc. Divisions requesting to create a new Social Media site must coordinate through the Office of Public Affairs (OPA). OPA involvement and monitoring ensures appropriateness and consistency of the message.

c. Publishing is controlled through designated PIOs that have received job specific training. The PIO coordinates with department staff.

d. Postings are required to be relevant, timely and actionable, and guidelines are provided to ensure sensitive or confidential information, as well as other protected communications (i.e. HIPAA) are not posted.

e. Instructions on how to provide links to pertinent data are included.

f. Comments are monitored to ensure they relate to FC business, rather than creating a public forum. Comments may be removed based on specific criteria, not because someone disagrees with County policy. Inappropriate comments include vulgar language, personal attacks, discriminatory remarks, spam, etc. Publishers are expected to respond to comments in a professional manner.

g. The policy links to a Photo / Video Release Form.

h. Specific directions are provided for Facebook, Twitter, YouTube, Flickr, and SlideShare.

i. Additional sections cover promoting government Social Media, how other Social Media opportunities may evolve, archival and records retention in compliance with Virginia law, information security including password complexity and notice that failure to follow set standards may result in disciplinary action and removal of the Social Media page(s).

j. Employees are prohibited from accessing Social Media sites while at work; however certain selected staff members may access Social Media for business purposes.

k. Employees are reminded they are personally responsible for content on their Social Media sites, blogs, etc. Employees are expected to speak for themselves and not to speak as officials for the government. If the employee chooses to publish data on any website that relates to their work, they must include a disclaimer that the content doesn't represent Fairfax County. Sensitive data may not be posted. Official seals connected to Fairfax County may not be posted.

l. The policy mentions that "friending" and "liking" can be potentially misinterpreted and may cause problems. Specifically mentioned are supervisor / subordinate relationships.

m. Violations of policy may result in disciplinary action.

B. Notable sections:

a. Modifications to the SOP require review by the E-Government Steering Committee, indicating the desire to maintain consistency across FC government.

b. A blog is available to release information during emergencies. The blog is controlled by the Office of Public Affairs.

c. Section I-E. provides clear guidelines on when comments may be removed. Inappropriate comments are retained via screenshots then deleted.

d. During emergencies, all Social Media content and postings must be coordinated through OPA.

<u>City of Houston Police Department – Police Agencies Use of Social Media – Literature Review</u>

A. Literature Review covers:

a. The definitions section defines Social Network and Social Media.

b. Social media successes of other police organizations are briefly described. Arlington, Texas P.D. hosts "tweet-alongs". Boston Police are using a crime tip texting program and a Twitter campaign. Dallas is using www.nixle.com to send out text messages and email alerts about neighborhood crime, traffic problems, community events, etc. Philadelphia Police launched a mobile version of their website that uses GPS to share the nearest police precinct. Seattle P.D. Tweets by beat.

c. Houston incorporates Social Media by using Facebook, Twitter, an interactive police blog, YouTube, podcasts, the department's web page, online reporting, and by publication of active police and fire incidents through the department's CAD system.

District of Columbia – Metropolitan Police Department Wide Area Network (MPDNet)

A. SOP Includes in part:
   a. The intent of the policy is to provide guidance on regulations and procedures governing MPDNet assets and services.
   b. The definitions section provides definitions for Computer System, Downloading, Hardware, Internet, Litigation Hold, Members, MPDNet, Obscene, Social Media, Social Networks and Software.
   c. Members may only access hardware and software they are authorized to access. Members may not install software, alter hardware, etc. Employees may use the Internet in an incidental fashion while not interfering with MPD computer assets, or interfering with their obligation to the MPD or D.C. Government.
   d. Provides guidelines on MPD's email account that require logging in on work days, responding to requests, password confidentiality, lack of privacy on MPD's network, handling of sensitive data, restriction of use of MPD's email system for union business and email retention.
   e. Internet usage is discussed for official business. Email and Internet prohibitions are discussed in detail.
   f. Personal Social Networking is discussed. Members may not post sensitive and / or confidential photographs or information, or information that would bring discredit on the MPD. An officer safety concern is raised regarding posting personal information, photos in uniform or postings of photos of MPD's vehicles and weapons.
   g. Professional Social Networking is allowed with permission of a commanding officer. Content must relate to performance of official duties and must remain separate from personal social networking accounts.
   h. Help desk details, supervisory duties and responsibility for violations are covered.

B. Notable sections:
   a. Section IV – 2 provides guidelines for professional social networking.

Minneapolis Police Department– Communications SOP AND Social Media Policy

A. SOP Includes in part:
   a. The Minneapolis Police Department (MPD) communications policy covers various issues related to police communications, including prioritization of calls for service, call number assignment, use of radio communications for police duties, notifications of command staff and other related content.
   b. Social Networking is discussed in Section 7-119. The term Social Networking Websites is defined.
   c. Employees are advised that MPD will monitor these websites and employees should use caution and good judgment when engaged in

social networking. The possibility of subpoena of content for civil or criminal matters is discussed.

d. Discipline may result if employees create posts that identify them as an employee of MPD, or make posts that are offensive or amount to unethical conduct. Employees are prohibited from speaking or acting on behalf of MPD, as well as indicating they are representing the interests of MPD. Employees may not use social networking to harass or attack others, including co-workers.

e. MPD has a standalone policy addressing Social Media as well. The policy describes how the City of Minneapolis formally participates in external Social Media communities.

f. The definitions section includes definitions for Employee, Social Media, Communications Department's Social Media Sites, Department Social Media Site and City's Social Media Sites.

g. The Communications Department (CD) takes a lead role in managing official business regarding Social Media. Departmental Social Media sites may only be created following approval by the Communications Department.

h. Employees are reminded that content will be monitored by the CD and they must conduct themselves in a professional manner when representing MPD on official Social Media sites. Only employees authorized to do so, may indicate they are representing or presenting the interests of the City.

i. Roles and responsibilities are outlined for the Communications Department, other departments, the City Attorney's Office and the Human Resources Department.

B. Notable sections:

a. There is a requirement that City Social Media sites link to the Official City of Minneapolis Website.

b. A prohibition against political campaigning on City Social Media sites is included.

c. Employees are prohibited from using the City's Social Media site to transmit information protected by a copyright, or is owned by another entity, without the owner's permission.

d. Consideration for disabled citizens is made evident by a stated desire to comply with the ADA, and to ensure disabled persons can receive crime alerts with commercially available text-based screen reader software.

<u>Montgomery County Maryland Police Department– Administrative Procedure 6-8, Social Media</u>

A. SOP Includes in part:

a. The purpose of the Social Media policy is to enhance communication, information exchange and collaboration with the public, regarding County programs, services and activities.

b. Department heads determine a department's official participation and representation on Social Media. Department heads coordinate through the Public Information Office. Department heads establish and maintain written rules about who may administer any departmental Social Media site.
c. Naming conventions and Social Media site appearance is discussed. The PIO has authority to modify and develop new standards to ensure consistency and credibility.
d. Legal requirements are discussed, including trademark and copyright concerns, privacy concerns, posting of preliminary documents and publishing of reports related to legal matters.
e. Employees are prohibited from making posts that endorse commercial products or services, make political endorsements, use County identifiers in connection with private enterprise, leverage County prestige for private gain, or violate policy.
f. Postings must comply with ADA accessibility requirements.
g. Guidelines for obtaining photo releases are included.
h. Guidelines for linking to or not linking to other web sites are included.
i. Roles and responsibilities are outlined for the Department Head, Public Information Office, Department of Technology Services, Office of the County Attorney and departments.

B. Notable Sections:
a. Governmental postings require the site administrator to identify themselves and provide their county email address as an avenue for follow up.
b. Publicly accessible Social Media sites are not the appropriate medium to communicate County policies to County employees.
c. If the Social Media site sells advertising or permit video displays, a delineated disclaimer must be included via a link or added to the home page.
d. If the site allows public comments, a delineated disclaimer is required. Retention of public comments, not in compliance with forum rules is discussed. Legal counsel must be consulted before deleting posts.
e. If the site links to other web sites, a delineated disclaimer is required.

<u>Nassau County Police Department – Social Media Policy AND Standards of Conduct</u>

A. SOP Includes in part:
a. The policy recognizes the value of using technology, internally for training and information acquisition and externally for dissemination of information to the public to include recruitment information, safety education information and for public relations purposes.
b. All Social Media pages shall be approved and shall adhere to applicable laws, regulations and policies, including records retention requirements.
c. Privacy concerns are discussed as well as restrictions on releasing confidential information.

d. Speech that impedes the performance of the department, undermines discipline and harmony among members, or creates a negative public perception of the department is prohibited.
e. The department maintains ownership of the network and data, and employees are reminded that communications may be monitored for appropriateness.
f. Nassau County Police have a separate Standards of Conduct policy that governs conduct when making electronic posts.

B. Notable sections:
  a. Records retention is discussed.

Philadelphia Police Department – Social Media and Networking

A. SOP Includes in part:
  a. Philadelphia Police endorse the secure use of social media to enhance communication, collaboration, and information exchange, streamline processes and foster productivity.
  b. The definitions section includes definitions for Social Media, Social Networking, Internet, Post (noun and verb), Blog and Comments.
  c. Employees are required to adhere to all federal, state and local laws, governing policies and laws specifically dealing with public information regarding arrests, investigations and personnel data.
  d. Employees may not connect their status as members of the police department in conjunction with product and service endorsements. Departmental property may not be used to engage in personal social media.
  e. While on duty, employees may not engage in personal use Social Media, using privately owned devices. While off duty, employees may only represent themselves and their personal interests when using Social Media.
  f. Social Media postings may lack privacy and may be obtained for use in criminal or civil proceedings, as well as departmental investigations.
  g. Employees may not use content that would be inappropriate in the workplace; nor may they post information in violation of the sexual harassment policy.
  h. Guidelines are provided for department authorized use of Social Media and personal use of Social Media.
  i. Internal use guidelines include requirements for participating in Social Media and prohibitions include making statements about a suspect 's or arrestee's guilt or innocence, comments concerning pending prosecutions and release of confidential information without the express written

permission of the Police Commissioner or designee. Conducting political activities or private business is prohibited.

j. External (personal) users may not represent or speak on behalf of the department. Posting of official seals are prohibited, including images of the city seal, police department badges, logos, patches or vehicles.

B. Notable sections:

a. Recognition is made that the personal use of social media may impact the department as a whole as well as members serving in their official capacity. Employees should always consider themselves as ambassadors for the department.

b. Employees may not post images of police personnel working in an undercover assignment or identifying these employees as officers.

c. Employees may not make personal Social Media postings where they are brandishing weaponry, contraband, tactical instruments and mechanical restraints.

San Francisco Police Department – Fraternization & Social Networking Policy

A. SOP Includes in part:

a. Anti-fraternization guidelines are discussed.

b. Members that interact on social networking sites shall conduct themselves at all times, in such a manner as to reflect most favorably on the department.

c. Documents that belong to the department may not be posted without the express written permission of the Chief of Police.

B. Notable sections:

a. Members may not post images of departmental property, equipment or personnel that may tarnish or demean the Department’s core values.

Seattle Police Department – Social Networking Sites Directive AND Standards & Duties

A. SOP Includes in part:

a. The Social Networking Sites Directive reminds employees that postings on Social Media may lack privacy and potentially create a permanent record of personal information. Information is being gathered by attorneys for civil and criminal litigation and criminal gang members are gathering intelligence from these same sites. Potential employers mine Social Media for information on job applicants. Employees are instructed to avoid posting language that may diminish the morale of Department employees and/or would adversely affect public confidence in the Department’s performance. Personal liability for postings is discussed.

b. The Standards & Duties policy, among several other regulations, prohibits employees from publicly criticizing or ridiculing the Department, its policies, other employees, other law enforcement agencies, the criminal justice profession, or the police profession, where such expression is defamatory, obscene, unlawful, undermines the effectiveness of the Department, interferes with the maintenance of discipline, or is made with reckless disregard for the truth.

B. Notable sections:

a. The Social Networking Sites Directive includes the following simple but meaningful quote, "If you don't want an employer or others to see what you're posting, don't post it!"

Virginia Beach – Information and Communications Technology Acceptable Use AND Facebook Terms of Use

A. SOP Includes in part:

a. The policy provides regulations regarding hardware and software, IT security, appropriate and inappropriate usage and accountability for use.

b. Users are required to abide by contractual provisions, federal, state and local laws and rules and regulations.

c. Prohibitions include transmission of inappropriate material based on content or copyright.

d. The definitions section includes definitions for Acceptable Use Policy, Authorized User, Cracking, Internet, Network or Networks, Information and Communications Technology Systems and User.

e. The City of Virginia Beach on Facebook – Terms of Use document indicates the purpose of their Facebook page is to provide local citizens with information about government programs, events and services, and to provide a platform for local citizens to share thoughts, opinions and suggestions about topics affecting the City of Virginia Beach.

f. A criterion for posting information on a City of Virginia Beach's Social Media page includes a statement that recognizes and encourages discussion and different viewpoints, and prohibits certain postings such as advertisements, nudity or pornography, personal attacks, and attacks on ethnic, racial, gender or religious groups.

B. Notable sections:

a. No expectation of privacy exists. Communications may become official business documents. Users are cautioned from including confidential or personal information in electronic media.

Honolulu Police Department – Organization, Management, and Administration – Social Media

A. SOP Includes in Part:

a. Employees are expected to maintain professionalism and uphold the integrity of the Honolulu Police Department (HPD), both while representing the department officially and while using Social Media for personal use.

b. The definitions section includes definitions for Blog, Bulletin Board/Message Board, Employee, Internet, Profile, Post, Social Media, Social Networks, Speech and Website.

c. The Chief of Police or designee may authorize the use of Social Media networks or sites, to any employee to promote the HPD's mission and goals.

d. Department authorized HPD social media shall include an indication they are maintained by the department, shall list departmental contact information prominently, include a disclaimer that visitor opinions are not the opinion(s) of the department and the department may remove postings that violate federal, state or local law, departmental rules and regulations, to include obscenities, commercial postings and political statements or endorsements. A link will be included on HPD Social Media pages to HPD's official web page.

e. Employees are reminded their speech becomes part of the World Wide Web and they are required to adhere to applicable rules and policies when using Social Media. Official postings must be respectful, professional and truthful.

f. Employees may express themselves as private citizens during personal use of social media. Postings must be legal, may not impair working relationships of the HPD, impede the performance of duties, impair discipline and harmony among coworkers, or negatively affect the public perception of the department. Confidential information may not be divulged and postings may not appear to represent the official position of the HPD.

g. Employees may not post speech inappropriate speech, such as obscene or sexually explicit language, nor may they make posts about themselves or other employees that embarrass or cause disrepute to the HPD. Employees may not post departmental symbols that would lead the user to believe the Social Media site is an official HPD site.

h. Employees should have a reasonable expectation that information posted in a public online forum may be accessed by the department at any time. Speech may also be used as grounds to undermine or impeach an employee's testimony in civil or criminal proceedings.

B. Notable sections:

   a. Corrections must be issued in the event incorrect data is issued on a HPD Social Media site.
   b. Officers working in undercover operations are prohibited from posting any visual or personal identification to any Social Media network which identifies them as an employee of HPD, or could compromise departmental objectives, or place someone else in danger.
   c. Employees may not post speech involving on-duty conduct of themselves or another employee reflecting behavior that would be considered irresponsible or reckless.
   d. Employees may not authorize, facilitate, distribute, or request that any third party display or post any images or comments involving himself or herself that would violate the requirements of employee's engaged in personal Social Media usage. Employees must make reasonable efforts to remove inappropriate third party postings on a social network under the employee's control.

Fort Worth Police Department – DRAFT Social Media AND City of Fort Worth – Use of Social Media For Official City of Fort Worth Business

A. SOP Includes in part:

   a. The draft SOP recognizes that personal use of Social Media may affect departmental personnel in their official capacity.
   b. The definitions section includes definitions for Blog, Page, Post, Profile, Social Media, Social Networks and Speech.
   c. Employees may express themselves as private citizens on Social Media sites to the degree their speech does not impede the performance of duties, impair discipline and harmony among coworkers, or negatively affect the public perception of the Fort Worth Police Department (FWPD).
   d. If an employee has a personal website that identifies the employee as being a FWPD officer, the employee must monitor and remove any postings that may bring an unfavorable impression of the employee or police department.
   e. The City of Fort Worth's Use of Social Media for Official City of Fort Worth Business policy recognizes the importance of Social Media for engaging citizens, to further the goals of the city and to better communicate with citizens in a real-time format.
   f. The definitions section includes definitions for Electronic Record, Moderator, Public Information, Social Media, Social Media Content, Social Networking and User.

g. Roles and responsibilities are delineated for the Office of Media and Public Affairs (OPMA), the Information Technology Solutions Department, departments, moderators, authorized users, public information officers and city employees.
h. For Social Media accounts that allow public posting and / or two-way communication, a delineated disclaimer is required.
i. The City's policy is accompanied by a Frequently Asked Questions document that answers general and technical questions about implementing and using Social Media.

B. Notable sections:
   a. Officer safety and security is an identified concern. Employees are cautioned not to disclose their employment with the FWPD and they may not post information pertaining to any other employee without their permission. Employees are cautioned not to post departmental symbols, including the badge and patch of FWPD, and they are additionally cautioned to not post personal photographs that may identify them as police officers.
   b. In the City policy, instructions are included when departments choose to close a Social Media account. They recognize the OMPA and / or department PIO may need to inform the public about the closing of the Social Media account.

APPENDIX AND RESOURCES

APPENDIX I

1. For the purposes of this survey, the term “social media” includes interactive electronic communication, as found in platforms such as Facebook, Twitter, YouTube, Pinterest, LinkedIn, etc. The nature of the communication may be instant messaging or online chatting, blogging, text messaging, transmitting phone videos or audio recordings or simply posting text on a social media tool. Please do not refer to routine email communication in responding to the questions provided below. POLICY Which of the following statements best describes your organization’s policy for social media in terms of policy oversight:

	Response Percent	Response Count
We do not have a policy that addresses any aspect of social media (skip to page 2).	5.3%	1
The city/county provides the overarching policy for the organization and the police department has a companion policy.	**52.6%**	**10**
The city/county provides the policy for the organization and the police department does NOT have a separate policy on social media.	0.0%	0
The city/county does NOT provide a policy for the organization, but the police department does have its own separate policy on social media.	10.5%	2
Other (please specify)	31.6%	6
	answered question	**19**
	skipped question	**0**

2. Which of the following statements best describes your organization’s policy for social media in terms of policy application?

	Response Percent	Response Count
The policy applies to all employees.	**100.0%**	**19**
The policy applies to sworn employees only.	0.0%	0
answered question		**19**
skipped question		**0**

3. Which of the following statements best describes the purpose/intent of your organization’s policy for social media?

	Response Percent	Response Count
The policy focuses on what actions are prohibited.	26.3%	5
The policy addresses both what actions are prohibited and the organization’s plan/strategy for utilizing social media to enhance effective communication and community relations.	**52.6%**	**10**
Other (please specify)	21.1%	4
answered question		**19**
skipped question		**0**

4. Which of the following statements best describe the scope of your organization's social media policy?

	Response Percent	Response Count
The policy addresses internet/email usage, but does NOT specifically address the use of social media such as Facebook, Twitter, etc.	21.1%	4
The policy provides a comprehensive discussion of internet, email and social media usage.	**78.9%**	**15**
answered question		**19**
skipped question		**0**

5. Specifically, which forms of social media does your department actively utilize and for what purpose?

	Recruiting	Community Outreach and Information (Programs & Events)	Citizens Reporting Crime	Public Safety Information Dissemination	Emergency Planning	Rating Count
Facebook	87.5% (14)	**100.0% (16)**	25.0% (4)	**100.0% (16)**	37.5% (6)	16
Twitter	50.0% (8)	87.5% (14)	18.8% (3)	**100.0% (16)**	43.8% (7)	16
YouTube	61.5% (8)	**84.6% (11)**	7.7% (1)	**84.6% (11)**	7.7% (1)	13
Text alert system	0.0% (0)	55.6% (5)	44.4% (4)	**88.9% (8)**	55.6% (5)	9
Smart Phone/ Tablet Applications (e.g. Crime Solvers app)	0.0% (0)	33.3% (2)	33.3% (2)	**50.0% (3)**	**50.0% (3)**	6
					Other (please specify)	7
					answered question	**19**
					skipped question	**0**

6. In thinking back over the past two years, describe department-wide successes and concerns relating to social media. Successes: (For example, a success might be promoting positive community relations through utilizing social media or seeing a surge of citizen participation in providing information regarding crime.)

	Response Count
	19
answered question	**19**
skipped question	**0**

7. Concerns: (A concern might be difficulties in controlling the timing of information being released or the release of inappropriate information. For the concerns, please respond how the situation was resolved, if possible.)

	Response Count
	19
answered question	**19**
skipped question	**0**

8. Do you provide training to employees regarding social media policies and appropriate use of social media?

		Response Percent	Response Count
Yes		42.1%	8
No		**57.9%**	**11**
		answered question	**19**
		skipped question	**0**

9. If you responded "yes" to the previous question regarding providing training to employees, please provide a description of the training provided (# hours, when provided to the employee, who provides the instruction, etc.):

	Response Count
	9
answered question	**9**
skipped question	**10**

10. Would you consider the use of social media by employees both on and off duty to be a concern for your organization?

	Response Percent	Response Count
Yes, both on and off duty	**84.2%**	**16**
Yes, but ONLY on duty	0.0%	0
No	15.8%	3
answered question		**19**
skipped question		**0**

11. Over the past two years, what percentage of disciplinary actions would you estimate resulted from the inappropriate use of social media?

	Response Percent	Response Count
None. We have not disciplined for inappropriate use of social media	31.6%	6
Less than 2%	**63.2%**	**12**
2 – 25%	5.3%	1
26-50%	0.0%	0
51-75%	0.0%	0
76–100%	0.0%	0
	answered question	**19**
	skipped question	**0**

12. What employee behaviors are you experiencing? Check all that apply.

	Response Percent	Response Count
Release of sensitive or confidential information about crime or other official police business	36.8%	7
Comments which may support an allegation of a hostile work environment	10.5%	2
Unprofessional representation of the department to the public	**63.2%**	**12**
Other (please specify)	57.9%	11
	answered question	**19**
	skipped question	**0**

13. What actions have you taken to address concerns regarding discipline trends related to employees' inappropriate use of social media?

	Response Count
	19
answered question	**19**
skipped question	**0**

14. What citizen interactions with your department are provided through social media? Please be specific about the social media tool and how it is used.

	Response Count
	19
answered question	**19**
skipped question	**0**

15. What is the expectation for response to citizen inquiries using social media?

	Response Percent	Response Count
Immediate – within the hour	10.5%	2
Same day (24 hour response)	26.3%	5
Only provided during standard business hours, Monday through Friday	26.3%	5
Other (please specify)	**36.8%**	**7**
answered question		**19**
skipped question		**0**

16. Who provides the response when citizens utilize social media?

	Response Percent	Response Count
Public Information/Media Relations Officer	**73.7%**	**14**
Internal Affairs	0.0%	0
Department Webmaster	0.0%	0
Dispatch	0.0%	0
Other (please specify)	26.3%	5
	answered question	**19**
	skipped question	**0**

17. What trends have you seen since the introduction of social media, particularly as it relates to community relations, crime reporting, public safety information dissemination and emergency planning?

	Response Count
	19
answered question	**19**
skipped question	**0**

18. If you use a social media dashboard (such as TweetDeck), please describe what you use and how you use it.

	Response Count
	19
answered question	**19**
skipped question	**0**

19. How do you measure the effectiveness of your social media tools?

		Response Count
		19
	answered question	19
	skipped question	0

20. Please provide contact information (name, department, email and phone number).

		Response Count
		19
	answered question	19
	skipped question	0

Page 1, Q1. For the purposes of this survey, the term “social media” includes interactive electronic communication, as found in platforms such as Facebook, Twitter, YouTube, Pinterest, LinkedIn, etc. The nature of the communication may be instant messaging or online chatting, blogging, text messaging, trans...

1	Our City and departmental policies address computer acceptable use in terms of maintaining privacy and security. Social media is not specifically addressed.	Feb 24, 2013 3:20 PM
2	SLCPD has drafted its own policy and is considering, wity adjustments, adopting the IACP model policy.	Feb 21, 2013 7:07 PM
3	Fairfax County Police Department is currently constructing a social media policy.	Feb 21, 2013 6:36 PM
4	No current policy in place, currently a draft form.	Feb 20, 2013 4:00 PM
5	We currently have a draft policy.	Feb 14, 2013 10:48 AM
6	The city of Raleigh has policy regarding the overall use of the Internet (not specific to social media) and a separate policy regarding a user agreement for the use of the computer and computer related equipment/ technology	Feb 11, 2013 8:21 PM

Page 1, Q3. Which of the following statements best describes the purpose/intent of your organization’s policy for social media?

1	The current policy reiterates that the same rules that apply in the real world apply in the virtual. By adopting the IACP model policy, with modifications, we hope to embrace a more guidance-oriented and best practices policy.	Feb 21, 2013 7:07 PM
2	The social media policy is currently under construction so the statement of purpose and scope are yet to be established or approved.	Feb 21, 2013 6:36 PM
3	No Policy	Feb 19, 2013 7:20 PM
4	The policy speaks general expectations if the Internet and general aspects of prohibited conduct.	Feb 11, 2013 8:21 PM

Page 1, Q5. Specifically, which forms of social media does your department actively utilize and for what purpose?		
1	"The Source" (www.milwaukeepolicenews.com)	Mar 1, 2013 12:22 PM
2	We do not use social media for any departmental activity. Box is checked to enable survey to go through but does not apply.	Feb 28, 2013 9:40 AM
3	Annoymous tip LIne- citizens reporting crime, Email List Serves- Used for Recruiting, community outreach, Public safety MRecrio	Feb 25, 2013 4:40 PM
4	Recruiting also uses Google and LinkedIn	Feb 22, 2013 2:10 PM
5	Pinterest, Instagram, Twitter; plus claiming our real estate on other SM platforms so others don't misuse it in our name -- some of that can be automated	Feb 21, 2013 7:07 PM
6	Yahoo Listserv	Feb 19, 2013 7:20 PM
7	Stop Houston Gangs.org and HPD Monthly Podcast	Feb 19, 2013 9:58 AM

Page 1, Q6. In thinking back over the past two years, describe department-wide successes and concerns relating to social media.
Successes: (For example, a success might be promoting positive community relations through utilizing social media or seeing a surge of citizen participation in providing informa...

1	The use of social media has allowed us to tell our side of the story instead of having a one-sided story. Social Media has also helped up publicize the good things our Agency does for the community.	Mar 7, 2013 12:49 PM
2	Our largest success has been with the posting of crime surveillance videos (on YouTube) depicting suspects. This has lead to the identification of numerous suspects and the solving of crimes.	Mar 1, 2013 12:22 PM
3	n/a	Feb 28, 2013 9:40 AM
4	MPD successfully closed robbery cases in part due to the videos mpd posted on YouTube. List Serves/email discussion groups allow mpd outreach teams to share informaton within the police districts and across the city. List Serves also allow for quick dissemination of informatio to large groups. Citizen response has been very positive particularly as it relates to posting patterns of criminal behavior on the list serves to keep the public aware of what is going on in their respective communities. Agency receives daily crime tips from members of the public through the list serve and the text a crime social media programs.	Feb 25, 2013 4:40 PM
5	Effective means of getting information out to public (e.g. jet crash in April 2012), publicizing job openings, promoting departmental activities like the citizen's police academy.	Feb 24, 2013 3:20 PM
6	1. Brings visibility to our large number of supporters. Our social media participants often post anecdotes of positive and heroic interactions with officers. When negative stories or comments are publicized, our participants have a forum to respond to those in a supportive way. 2. A place to "get the story straight" when professional media outlets don’t report the whole story. 3. Day-to-day positive stories which the media does not have time to report can be published. Citizens often report feeling safer in their neighborhoods after hearing of effective police work. 4. Services, events and programs can be highlighted. Our heavy community outreach and large citizen volunteer involvement means there's always something to announce or celebrate. 5. Citizens can ask questions and get timely, no-hassle answers or referrals. 6. Very successful for recruiting for the academy, citizen volunteering and youth programs. 7. Recently, we held a joint "Tweetalong" with Arlington Police Department. We tweeted what it feels like to ride out with an officer. APD retweeted our comments and vice versa. Other departments around the nation also followed us and gave us a great sense of connection not only to the citizens following and participating, but also to our colleagues in law enforcement in other cities. This event is great for providing the experience to anyone who could not participate in a real ride along with an officer. It gives a greater number of persons the experience, without as many safety concerns to either the citizen or the officer.	Feb 22, 2013 5:17 PM
7	Social media provides more interaction with the community. Allows for a 24/7 conversation with the community. We have had success in locating missing persons and solving crimes in neighborhoods with the help of social media.	Feb 22, 2013 2:10 PM
8	We've recently embraced a tweet-along concept for holiday DUI saturations. It was a success in communicating the level of DUI activity, but also attracted the	Feb 21, 2013 7:07 PM

Page 1, Q6. In thinking back over the past two years, describe department-wide successes and concerns relating to social media.
Successes: (For example, a success might be promoting positive community relations through utilizing social media or seeing a surge of citizen participation in providing informa...

	naysayers who feel DUI saturations ruin lives and fill city coffers. Once reasonable people started challenging them, those folks went away. Twitter has by far been our most successful SM platform -- enabling the timely dissemination of information, reTweets of emergency information around the valley (especially during natural disasters like fires and floods), and is generally increasing the 2-way conversation. The biggest obstacle to successful SM engagement is the need for Admin/supervisors to understand staffing needs and consistent application -- not to mention that SM is NOT a communications panacea, rather it's just another tool in an integrated communications and outreach plan that must be continually updated.	
9	Internal assessment and discussion which will develop this information pursuant to the construction of our social media policy is pending.	Feb 21, 2013 6:36 PM
10	Use of the Department's Webpage and tip line.	Feb 21, 2013 3:27 PM
11	The Philadelphia Police Department is enjoying great success using social media. According to IACP, we have the most popular Facebook page of any municipal law enforcement agency in the United States. Our efforts have been profiled by many publications such as NPR, ABC National News, Government Tech magazine and many more.	Feb 21, 2013 2:40 PM
12	Successes for Honolulu PD include: being able to establish a link to Facebook posting Hawaii's Most Wanted information. Current interconnection with our website allows for posting of traffic lane closures, and updated traffic related information to assist motorists. Our department assigned fulltime personnel to a "Virtual Unit".	Feb 20, 2013 4:00 PM
13	n/a	Feb 20, 2013 1:05 PM
14	Use of social media has enhanced our relaionship with the communuity by allowing a timely dissemination of information and a timely response to citizen inquires.	Feb 19, 2013 7:20 PM
15	HPD has successfully used social media to provide information to the community regarding crime prevention methods and tools, information on upcoming events the community can become involved in (i.e. National Night Out and the department’s annual food drive) and has also spotlighted officers in a recurring post called “Officers In Action” which summarizes officers that have been commended for their outstanding work. Through all these measures HPD has been able to engage the public in a way that was previously not accessible. The implementation of a Facebook page, twitter feed and monthly podcast have all reached various audiences that were previously not reached. HPD also worked jointly with other surrounding agencies to implement a Stop Houston Gangs website which has been very successful in getting wanted gang members off the streets and arrested and has allowed the public to provide tips in cases which have led to hundreds of arrests.	Feb 19, 2013 9:58 AM
16	Our biggest successes have been the ability to push out our own media and information without relying on traditional news outlets. For example during the	Feb 14, 2013 12:28 PM

Page 1, Q6. In thinking back over the past two years, describe department-wide successes and concerns relating to social media.
Successes: (For example, a success might be promoting positive community relations through utilizing social media or seeing a surge of citizen participation in providing informa...

	last recruitment drive for the position of police officer the N.C.P.D had twenty thousand applicants sign up for the exam. We feel that social media played a large role in this success of this recruitment drive	
17	With twitter we are able to get information out before the media.	Feb 14, 2013 10:48 AM
18	Getting info to community quickly	Feb 12, 2013 7:09 PM
19	All personnel have had a 4 hr block of in- service training which specifically addresses social media... This participatory training required classroom exercises, debates on the pros/ cons and consequences of using social media while addressing the intel uses; the reality of criminals also using it to follow law enforcement; the use if attorneys using it against officers in court because of things the officers have tweeted or placed on their Facebook or my space pages.	Feb 11, 2013 8:21 PM

Page 1, Q7. Concerns: (A concern might be difficulties in controlling the timing of information being released or the release of inappropriate information. For the concerns, please respond how the situation was resolved, if possible.)		
1	Our biggest concern is finding a Public Information Officer that has the right skill sets to utilize social media to better the Agency.	Mar 7, 2013 12:49 PM
2	The information we release is generally vetted through numerous internal sources and once approved, the posting to the applicible social media is done primarily by the PIO. For this reason, we do not have a great concern of unauthorized information being shared.	Mar 1, 2013 12:22 PM
3	n/a	Feb 28, 2013 9:40 AM
4	Citizens try to substitute list serves/texting and facebook to report emergencies that require 911 assistance. ListServes sometimes used inappropriately to insult others, submit links to businesses, disseminate false information; to lodge complaints against individuals police officers.	Feb 25, 2013 4:40 PM
5	Employee judgment in posting images including departmental vehicles, uniforms, etc.	Feb 24, 2013 3:20 PM
6	Although it appears to be a more casual and personal form, all the principals of good public information best practices should be in place at all times. Checks must be in place to prevent slander, privacy and civil rights violations and inaccurate information, for anyone involved or mentioned, including suspects, victims, citizens and police personnel. Information for social media must be geared to the venue. Social media followers are often not professionals and so things must be explained; jargon should be limited and defined. Things can be a little lighter than a straight media release, and certainly there needs to be a human and personal voice, however, jokes, sarcasm and quips usually backfire. Never forget that the audience is very broad and that this is the official voice of the Department. Decorum is always appropriate. Citizens are encouraged to respond to our posts and we try to provide a free and open forum. We set our profanity filters high, so that any post containing that will be hidden automatically. We do not permit advertising of products or services. We will take down posts that are not family-friendly. We do keep a record of every deleted or hidden post via a screen shot. At the FWPD, we send a proposed post or comment to others on the media relations team for review. Another pair of eyes can catch mistakes, red flags, etc. and sometimes are aware of relative issues, circumstances or information that could cause problems.	Feb 22, 2013 5:17 PM
7	Some of our concerns with regard to the use of social media has been the citizens who post negative information, dishonest information, and those that use bad language.	Feb 22, 2013 2:10 PM
8	Poster's remorse. Frequently we can get information out much faster than certain detectives realize. They change their minds about issuing certain photos or information but it's already out. Taking down a post, especially without explanation or archiving, is something we won't do. If it's out, it's out. We will correct, but not delete. We were unable to secure the same vanity brand -- slcpd -- across all SM platforms, which then requires a bunch of explaining. It would be much simpler to say, look for us on any major SM under the brand SLCPD. To work around that, we include SM icons on our website and in our email signatures that connect with a simple click. We also pull our Twitter feed into our	Feb 21, 2013 7:07 PM

Page 1, Q7. Concerns: (A concern might be difficulties in controlling the timing of information being released or the release of inappropriate information. For the concerns, please respond how the situation was resolved, if possible.)

	website, and hope to add more as we update www.slcpd.com. Admin/supervisors are not fully on board with supplying the proper tools that make the use of SM easy. Specifically, if an agency uses SM, all personnel responsible for its management should have the best smart tools available -- tablets, smart phones, etc. Admin/supervisors should not "short" their staff; it should be properly budgeted and expedited if they expect their personnel to succeed. No agency can use or populate every SM platform out there. As a result, the state of SM must be monitored for updates and efficacy, with the agency deciding what it can do with the resources it is willing to allocate. Another concern is integrating it into a website where an agency's IT department is reluctant to pull it in due to security concerns. A huge problem for us is that lack of customer service with Facebook. We started running before we could walk on this platform and would like to merge two pages while keeping our vanity ID and all of our friends/likes. This seems like a pretty simple thing that could be done, but they will not communicate directly on the topic. I'd like to see Facebook create a LEO ombudsman to help with such issues -- I know, dream on. Lastly, we need to go mobile -- mobile website, mobile applications. We lack budget and IT abilities to get it done.	
9	Internal assessment and discussion which will develop this information pursuant to the construction of our social media policy is pending.	Feb 21, 2013 6:36 PM
10	N/A	Feb 21, 2013 3:27 PM
11	Having 15 individual officers using Twitter, we have experienced information being released before the Public Information Officers were prepared to handle questions. With social media being an emerging form of police communications, small problems are to be expected and are fairly easy to deal with.	Feb 21, 2013 2:40 PM
12	Occasional concerns from investigative units regarding the amount of information released have arisen. Better coordination and communication between our Virtual Unit and the investigative units has alleveated most of the friction.	Feb 20, 2013 4:00 PM
13	n/a	Feb 20, 2013 1:05 PM
14	We have concern of the improper relase of information, so on our listserv a limited number of members has permissions set to post "un-monitored".	Feb 19, 2013 7:20 PM
15	The on-going concern is the use of negative comments involving profanity and disparaging remarks regarding officers. The Facebook page is monitored 24 hours a day and inappropriate comments are hidden. Some users, based on their comments and abuse of the page are also banned.	Feb 19, 2013 9:58 AM
16	The N.C.P.D. has Public Information Office that works twenty four hours a day; seven days a week. All information is vetted and controlled by the departments PIO office in accordance with our news release guidelines. Within PIO one detective is our social media director who is responsible for content, edits and review of our Facebook and Twitter accounts. So no real concerns within the N.C.P.D.	Feb 14, 2013 12:28 PM

Page 1, Q7. Concerns: (A concern might be difficulties in controlling the timing of information being released or the release of inappropriate information. For the concerns, please respond how the situation was resolved, if possible.)

17	Don't know	Feb 14, 2013 10:48 AM
18	Possible mistake in the release of inaccurate info	Feb 12, 2013 7:09 PM
19	We don't have any widespread concerns. Matters that are inappropriately are handled on a case-by-case basis.	Feb 11, 2013 8:21 PM

Page 1, Q9. If you responded "yes" to the previous question regarding providing training to employees, please provide a description of the training provided (# hours, when provided to the employee, who provides the instruction, etc.):

1	There is a one hour power point presentation provided to new officials with regard to the use of the List Serve/Email discussion groups. This is done by the Department's Community Outreach Coordinator. No other formal training exists. There is informal training by supervisors to subordinates but that is on a case by case as there is no department mandate for trainng, other than the list serves.	Feb 25, 2013 4:40 PM
2	We do provide internet security and privacy training during the recruit academy (2 hour class) but it focuses more on the acceptable us of City computers versus the appropriate use of social media. Our ComIT Department publishes a quarterly report for department directors which identifies the top 20 users and lists the websites that they visit.	Feb 24, 2013 3:20 PM
3	Our Training and Education Division provides training to police officer candidates within the new recruits classroom curriculum. Training and Education also provides a minimum of one hour training on social media to all sworn and civilian employees during annual in-service training.	Feb 22, 2013 2:10 PM
4	The criminal justice academy provides a basic training block of instruction to police officer recruits focussed on potential detriments in their person use of social media as they transition from civilian jobs to law enforcement. The criminal justice academy also provides full day in-service training by expert contractual instructors on defensible utilization of social media in background and criminal investigations.	Feb 21, 2013 6:36 PM
5	Training is provided before employees are permitted to represent the department on Twitter. The training is one day (8 hours) and it is conducted by the Public Affairs Unit.	Feb 21, 2013 2:40 PM
6	All classified personnel are required to take a four-hour course on the department’s social media policy and general do/don’ts for both on and off duty. The course is taught by HPD personnel responsible for managing the department’s social media communications. All officers will receive the training during the course of the 2012-2013 training calendar.	Feb 19, 2013 9:58 AM
7	The N.C.P.D. does provide formal training for all members of the department. The Commanding Officer of P.I.O. instructs officers and supervisors about dealing with the press and our policies and rules that govern social media. This is done during an hour long lecture at the police academy.	Feb 14, 2013 12:28 PM
8	Outreach coordintaor provides training to all supervisors	Feb 12, 2013 7:09 PM
9	The State of NC provides mandatory lessons in some subject matters...Ethics/ Career Survival in Social Media was the 2012 lesson. All sworn personnel received the same lesson throughout the state. I, Cassandra Deck-Brown, am the Ethics Instructor.	Feb 11, 2013 8:21 PM

Page 1, Q12. What employee behaviors are you experiencing? Check all that apply.		
1	Criminal behavior	Mar 7, 2013 12:49 PM
2	Our trouble has been primarily with Facebook, but some Twitter related concerns also.	Mar 1, 2013 12:22 PM
3	none at this time	Feb 28, 2013 9:40 AM
4	facebook comments/photos; "replying to all"	Feb 25, 2013 4:40 PM
5	Evidence of domestic issues in the private lives of both sworn and civilian personnel may be found in SM.	Feb 21, 2013 7:07 PM
6	The Commander of Internal Affairs Bureau provided input summarized in 13.	Feb 21, 2013 6:36 PM
7	None of these	Feb 21, 2013 2:40 PM
8	No adverse behaviors	Feb 19, 2013 7:20 PM
9	None at this time.	Feb 14, 2013 10:48 AM
10	Personal messages which are seen as unprofessional	Feb 12, 2013 7:09 PM
11	Comments, tags or photos on the employee's personal social media sites that are inappropriate & not reflective of agency's goals	Feb 11, 2013 8:21 PM

Page 1, Q13. What actions have you taken to address concerns regarding discipline trends related to employees' inappropriate use of social media?

1	Our internal policies and procedures have been updated. Invididual coaching has also taken place.	Mar 7, 2013 12:49 PM
2	To avoid these types of incidents, SOP is reinforced periodically through the publishing of reminder memos and/or Roll Call videos.	Mar 1, 2013 12:22 PM
3	none	Feb 28, 2013 9:40 AM
4	clarified the order; hold commander resolution conferences with employees; taken both corrective (official reprimand) to adverse action (suspension to removal) depending on the severity of the violation. egreg	Feb 25, 2013 4:40 PM
5	Disciplinary action. Revised definition of "Conduct Unbecoming" rule violation to include the inappropriate use of social media. Sent email reminders to employees citing court cases from other cities.	Feb 24, 2013 3:20 PM
6	We are expanding on our policy and procedures for social media. More of the instructors in our Academy note the positives of social media, as well as the negatives.	Feb 22, 2013 5:17 PM
7	Our Policy and Planning Division is currently working on a directive concerning the inappropriate use of social media. In addition, inappropriate use of social media is discussed at length during in-service training.	Feb 22, 2013 2:10 PM
8	Policy has been issued and it is reiterated as issues arise. We also are working on adapting the IACP model policy for our use.	Feb 21, 2013 7:07 PM
9	The Internal Affairs Bureau Commander responded that IAB's tracking system allows search by name and policy infractions, etc. Since no social media policy has been approved and disseminated, no cases are specifically tracked to a social media infraction. IAB staff were canvassed by the commander and staff noted that social media utilization had factored into some of their casework, but that it would require a hand search of case files to make the connections between tracked policy infractions and the social media issues uncovered during their investigations. The commander could not reasonably justify the hand search given the current case loads taking priority.	Feb 21, 2013 6:36 PM
10	N/A	Feb 21, 2013 3:27 PM
11	We are proactively training officers that use social media as part of their duties and we are working with the Pennsylvania Municipal Police Officers Training and Education Commission to develop social media training for all police officers, statewide.	Feb 21, 2013 2:40 PM
12	A draft policy has been created and is awaiting final approval. Commanders have been kept apprised of the issues regarding social media, and are expected to breif thier personnel.	Feb 20, 2013 4:00 PM
13	n/a	Feb 20, 2013 1:05 PM
14	N/A	Feb 19, 2013 7:20 PM
15	A department policy was issued to address the concerns in addition to the in-	Feb 19, 2013 9:58 AM

Page 1, Q13. What actions have you taken to address concerns regarding discipline trends related to employees' inappropriate use of social media?

	service training that has been implemented for all classified personnel.	
16	The N.C.P.D. has devolved a comprehensive social media policy and has amended our departmental rules to list prohibited actions.	Feb 14, 2013 12:28 PM
17	NA	Feb 14, 2013 10:48 AM
18	Issue discipline	Feb 12, 2013 7:09 PM
19	Training to all employees and the user agreement is signed annually as a reminder.	Feb 11, 2013 8:21 PM

Page 1, Q14. What citizen interactions with your department are provided through social media? Please be specific about the social media tool and how it is used.

1	We utilize Facebook and Twitter. The feedback/posts we receive from community members is not the same group of community members that normally would comment on our Agencies' performance. We are definitely reaching a wider audience and obtaining different feedback than we are used to.	Mar 7, 2013 12:49 PM
2	Generally, the commenting features are turned off (if applicable) to the social meida being used. We try and avoid the interactive mode, because we do not want to give the perception the public can notify our department of a crime through social media.	Mar 1, 2013 12:22 PM
3	none	Feb 28, 2013 9:40 AM
4	See attached word document.	Feb 25, 2013 4:40 PM
5	Through Facebook, we alert the public to traffic problems, solicit info regarding crime and provide info about programs and events. Essentially, information that was released via press release in the past is now posted to Facebook. Citizens may report crimes and retrieve crime reports through our website via ePro.	Feb 24, 2013 3:20 PM
6	This question has been answered on several points above. Citizens are encouraged to ask questions, tell us about their experiences with the FWPD, and participate in conversations on the topics we post. We use Facebook to tell the longer stories, give more detailed information and provide a more involved conversation. We usually limit our posts to one or two per day. Twitter has a short version or link to what is on Facebook, but we put things on Twitter that are not on Facebook	Feb 22, 2013 5:17 PM
7	On Facebook we post press releases, crime alerts, and locations of speed cameras which at times encourages citizen interactions. Citizens have also used Facebook to post comments on police conduct-both positive and negative.	Feb 22, 2013 2:10 PM
8	All of our public facing communications are copied on our SM channels, adapted appropriately for each platform or edited for dissemination via SM tools like Hootsuite. We have stayed away from creating multiple Facebook or Twitter pages due to limited resources. However, we are considering non-monitoried use dedicated to specific funcations, e.g., stolen car alerts, etc.	Feb 21, 2013 7:07 PM
9	Face Book postings in regard to programs, events, and awards. Twitter used to alert followers to crimes, developing incidents, road closures. Answers are generated to citizen questions received on Face Book and Twitter.	Feb 21, 2013 6:36 PM
10	Community Forums	Feb 21, 2013 3:27 PM
11	The PPD has a interacts with the public on all of the social media platforms in which we engage. Facebook, Twitter, Pinterest and YouTube are used to respond to questions from citizens and provide them with timely information.	Feb 21, 2013 2:40 PM
12	We've recieved tips regarding possible identities of wanted suspects via Facebook, in addition to providing answers to specific questions the public may have regarding department events, crime trends, or employment activities.	Feb 20, 2013 4:00 PM
13	facebook	Feb 20, 2013 1:05 PM

Page 1, Q14. What citizen interactions with your department are provided through social media? Please be specific about the social media tool and how it is used.

14	Through each police districts listserv we interact with citizens numerous times daily.	Feb 19, 2013 7:20 PM
15	On Facebook citizen comments are allowed on the posts, in addition we encourage our followers to share the information on their own Facebook pages. Comments are responded to and we encourage dialogue regarding the post. Recently HPD held a town hall meeting and encouraged questions to be submitted via Facebook and twitter. Commonly meetings and news conferences are tweeted in real time. During those instances, twitter feedback is responded to. On the Stop Houston Gangs website, viewers are encouraged to provide anonymous tips on the whereabouts of wanted suspects and provide confidential information on gang activity on gang activity they have knowledge of. HPD is also working on increasing the interactive function of twitter and other social media sites that will allow more two-way communication with the public and the department, including the implementation of Instigram and Pinterest. Both these tools should be fully utilized in the next 3-4 months.	Feb 19, 2013 9:58 AM
16	Most of the information in the N.C.P.D. is pushed out to our citizens. At this point we ask the public to contact us with information by traditional means.	Feb 14, 2013 12:28 PM
17	Don't know	Feb 14, 2013 10:48 AM
18	Listserv with the community	Feb 12, 2013 7:09 PM
19	1)We recruit using a Facebook page. Communication is two-way. 2) The city of Raleigh has a portal identified as "see, click, fix" the citizens throughout the city of Raleigh who identify areas of improvement or have questions or inquiries...they can simply email their concerns and they are forwarded to the appropriate department within city government to address so for instance I sent an email last week as a citizen because I noticed one of the neighborhood street signs was leaning and I didn't want it to fall on one of the kids while waiting for bus so I sent an email regarding the concern and the location and the next day the sign was re-erected and upright. 3) Citizens also have access to an email site within the Raleigh Police Department whereby they can direct specific police related concerns and a response is given provided it is an appropriate request. 4) Our intelligence center uses various forms of social media to surveil various activities by a particular groups that are of interest to the police department.	Feb 11, 2013 8:21 PM

Page 1, Q15. What is the expectation for response to citizen inquiries using social media?

1	n/a	Feb 28, 2013 9:40 AM
2	For the most part, responses to citizen inquiries are made during normal business hours, however public information officers respond to pressing issues as needed during off hours as well.	Feb 22, 2013 2:10 PM
3	During standard business hours AND during developing major incidents.	Feb 21, 2013 6:36 PM
4	The reponse is immediate (within 15 minutes) normally but accounts are monitored by one person so overnight and certain times on the weekends there can be a longer wait.	Feb 21, 2013 2:40 PM
5	n/a	Feb 20, 2013 1:05 PM
6	We ask citizens to contact the police department through 911, Crimstoppers Hotline or local precinct	Feb 14, 2013 12:28 PM
7	It is usually 24-48 hours. However, it does Depend on the gravity of the request	Feb 11, 2013 8:21 PM

Page 1, Q16. Who provides the response when citizens utilize social media?

1	n/a	Feb 28, 2013 9:40 AM
2	Watch Commanders, Lieutenants and Above for List Serves and Email discussion; public information and webmaster for responses as a result of mpd sending out general information or alerting the public on an issue.	Feb 25, 2013 4:40 PM
3	The department Virtual Unit, or if recruitment related, our Human Resources Division recruitment sergeant.	Feb 20, 2013 4:00 PM
4	Police Supervisors	Feb 19, 2013 7:20 PM
5	All supervisors	Feb 12, 2013 7:09 PM

Page 1, Q17. What trends have you seen since the introduction of social media, particularly as it relates to community relations, crime reporting, public safety information dissemination and emergency planning?

1	We are now reaching a much larger, diverse audience with information.	Mar 7, 2013 12:49 PM
2	Our local population has become more reliant on social media as a means to get information. We are constantly adapting to meet those needs, but we also find it is extremely burdonsome to keep up with technology and making sure all our platforms are updated timely.	Mar 1, 2013 12:22 PM
3	n/a	Feb 28, 2013 9:40 AM
4	Increased expectation that information will be provided to the public through a variety of social media tools; citizens seem to be more aware of the issues affecting their respective communites.	Feb 25, 2013 4:40 PM
5	The public has a greater expectations for information and for a timely response.	Feb 24, 2013 3:20 PM
6	Some LE agencies are using mass texting services for emergency management, but our EM unit handles that. We notice that some agencies tweet active calls, accidents, etc. One major city we observed did this at the beat level. One of the results was actually making citizens feel more nervous, knowing that their neighborhood was that active. We have decided not to report active calls, except during a publicized Tweetalong event. Our social media community responds to feature stories, follow-ups, crime preventions tips and other information with enthusiasm. When we repeat what we send to the professional media outlets for their crime beat reporting, our community points out the redundancy.	Feb 22, 2013 5:17 PM
7	We use social media to clarify or clear up any misconceptions the community may have regarding the police though it is a work in progress and we don't have a measurement of trends at this time. We don't encourage the use of social media for crime reporting as we still recommend calling 911. We receive positive feedback from the community regarding the use of text messages and facebook postings to disseminate public safety and emergency planning such as adverse weather conditions and accidents and/or police activity that affects traffic routes.	Feb 22, 2013 2:10 PM
8	The public expects to be able to contact us for service through social media, although our SM platforms have disclaimers to the contrary (that it's not a dispatchable point of contact). They also would like to be able to send text and video to Dispatch, although we are able to accept it through our Text-a-Tip service, I believe.	Feb 21, 2013 7:07 PM
9	Response to this item will be pending further progress in the construction of our social media policy.The tabulation on item 5 shows the extent of utilization by PIO on behalf of the entire agency, but trend analysis is lacking.	Feb 21, 2013 6:36 PM
10	Increased access to information	Feb 21, 2013 3:27 PM
11	The flow of information is more rapid and the public's expectation has increased dramatically. It also seems that departments that were not early adopters of social media are now scrambling to catch up.	Feb 21, 2013 2:40 PM
12	The public seems to respond quickly to information posted, whether it be for assistance in identifying possible suspects, on-going recruitment activities, or	Feb 20, 2013 4:00 PM

Page 1, Q17. What trends have you seen since the introduction of social media, particularly as it relates to community relations, crime reporting, public safety information dissemination and emergency planning?

	public safety information.	
13	n/a	Feb 20, 2013 1:05 PM
14	Great tool for communicating with the community; however, also less people attend community meetings because they already have received information through listserv.	Feb 19, 2013 7:20 PM
15	As HPD has increased their presence on social media sites, citizen interaction has increased, along with the positive perception of the department. It has allowed the department to embrace a new level of transparency and get our message out to the public in real time. Having an additional route to express our events in the community allows us to reach a perceptive, engaged audience. We have also embraced the use of tweeting for emergency planning. Often we will tweet information on road closures due to accidents in order to allow citizens to re-route their commutes. Last, we have had success using social media to post surveillance video and photos or sketches of wanted suspects. Oftentimes this makes the public aware of cases HPD is working and allows HPD to reach a different audience than regularly reached through traditional media.	Feb 19, 2013 9:58 AM
16	The N.C.P.D. has been using social media on a regular basis for the past eighteen months. It has become an invaluable tool for information dissemination and getting feedback from our citizens' particularly on Facebook. I would suggest that the social media director or his designee check the website frequently because some of the feedback is criticism which we understand will take place but other comments are quite derogatory and rude.	Feb 14, 2013 12:28 PM
17	Better relationships with the community.	Feb 14, 2013 10:48 AM
18	It works well, and the public expects it.	Feb 12, 2013 7:09 PM
19	Relationships are strengthened. It is an attempt to recognize that we need to communicate with the citizens and if social media is a means by which to do that then it's a necessary tool. It is important to realize that at times, there's a necessary dialogue which must occur face-to-face or by telephone rather than typing a message to someone. Spending too much time communicating via social media can be time-consuming. When time is of the essence, social media may not be the most effective or efficient means of communicating, it may require a conversation between two people.	Feb 11, 2013 8:21 PM

Page 1, Q18. If you use a social media dashboard (such as TweetDeck), please describe what you use and how you use it.

1	Do not use	Mar 7, 2013 12:49 PM
2	We used Tweetdeck until the end of 2012. Due to a 2013 position cut by the city council, we have lost the civilianized position of Media & Communications Manager. This person has oversight of this area of social media. The position has not been re-established and we have not been active in working this application.	Mar 1, 2013 12:22 PM
3	n/a	Feb 28, 2013 9:40 AM
4	N;/A	Feb 25, 2013 4:40 PM
5	n/a	Feb 24, 2013 3:20 PM
6	We use Twittus and Hootsuite and are trying out Sprout Social. Twittus automatically posts our Facebook posts to our Twitter account. We use Hootsuite to schedule posts for later to either or both Facebook and Twitter. We also use Hootsuite as a dashboard to monitor various elements of Facebook and Twitter	Feb 22, 2013 5:17 PM
7	N/A	Feb 22, 2013 2:10 PM
8	We have used several, but they tend to malfunction over time, at which point we'll switch to another. We are currently enjoying success using Hootsuite. We're able to post to both Twitter and Facebook in one stroke. A growing problem is that Facebook users don't like seeing hashtags in their Facebook posts, which then defeates the use of SM dashboard. We did just acquire Radian 6 as a media monitoring tool. I'm excited to see all it can do in the traditional and SM world.	Feb 21, 2013 7:07 PM
9	Hoot Suite is utilized to monitor a variety of streams and Face Book.	Feb 21, 2013 6:36 PM
10	N/A	Feb 21, 2013 3:27 PM
11	We use TweetDeck to follow certain feeds and send out tweets. Tweets are never scheduled and other platforms are used directly with no 3rd party software.	Feb 21, 2013 2:40 PM
12	None	Feb 20, 2013 4:00 PM
13	n/a	Feb 20, 2013 1:05 PM
14	N/A	Feb 19, 2013 7:20 PM
15	N/A	Feb 19, 2013 9:58 AM
16	N/A	Feb 14, 2013 12:28 PM
17	NA	Feb 14, 2013 10:48 AM
18	Listserv used everyday to convey and receive info	Feb 12, 2013 7:09 PM
19	N/A	Feb 11, 2013 8:21 PM

Page 1, Q19. How do you measure the effectiveness of your social media tools?		
1	We utilize the delivered social media analytics. Overall, the measurement of effectiveness is limited due to the skill sets of our current Public Information Officers.	Mar 7, 2013 12:49 PM
2	Interaction has been strong. Most of our effectiveness is determined by the number of hits and any information coming in that can be contributed to our social media use.	Mar 1, 2013 12:22 PM
3	n/a	Feb 28, 2013 9:40 AM
4	List serves/email discussion groups customer satisfaction commens and promotion of the list to other community groups; There is an agency and a citywide report card citizens can access and rate MPD on response time, interaction, information disseminated using social media tools.	Feb 25, 2013 4:40 PM
5	n/a	Feb 24, 2013 3:20 PM
6	Hootsuite, Facebook Insights, Google Analytics, trying out Sprout Social.	Feb 22, 2013 5:17 PM
7	We measure the effectiveness by how many "likes" we get on FaceBook; how many followers we get on Twitter; as well as the number of people who visit our website-MCP News.	Feb 22, 2013 2:10 PM
8	We look for retweet/like success, but to look at it in a standalone environment is misleading. As I said earlier, SM has got to be part of an integrated communications and outreach plan.	Feb 21, 2013 7:07 PM
9	Metrics are available in regard to Face Book, in regard to Tweets, and pertinent to the growth in followers on Twitter.	Feb 21, 2013 6:36 PM
10	In Progress	Feb 21, 2013 3:27 PM
11	We keep track of our followers on each platform. We also track the number of arrests made from criminal events where information was released via social media.	Feb 21, 2013 2:40 PM
12	By monitoring the amount of followers the deparment site recieves, and the analytics regarding the volume of activity the information provokes.	Feb 20, 2013 4:00 PM
13	n/a	Feb 20, 2013 1:05 PM
14	N/A	Feb 19, 2013 7:20 PM
15	Through the number of followers and fans on the respective pages, how often a post is shared or re-tweeted and the comments left on the page. Facebook insights stat page as well.	Feb 19, 2013 9:58 AM
16	The effectiveness of our social media is hard to quantify at this point. In 2013 we will begin to push out much more information to the public using social media. We also would like to development a Crime-Stoppers smart phone application which will allow our younger citizens to provide crime information without the anxiety of speaking to a detective on the phone.	Feb 14, 2013 12:28 PM
17	Don't at this time.	Feb 14, 2013 10:48 AM

Page 1, Q19. How do you measure the effectiveness of your social media tools?		
18	If the public thinks we are doing a good job	Feb 12, 2013 7:09 PM
19	Recruitment - We are asking applicants how would they made aware of the fact that we were hiring. PIO- We assess the use and the inquiries made via social media. Intelligence/investigations-Based on the value and credibility of the information we gather via those social media sites.	Feb 11, 2013 8:21 PM

Page 1, Q20. Please provide contact information (name, department, email and phone number).

1	Bryan Seboe HR Generalist Minneapolis Police Department (612) 673-2792 <bryan.seboe@minneapolismn.gov>	Mar 7, 2013 12:49 PM
2	Sgt. Mark Stanmeyer Milwaukee Police Department Media and Communications mstanm@milwaukee.gov	Mar 1, 2013 12:22 PM
3	Jennifer Ford, Lieutenant 1395 Washington Blvd Pittsburgh, PA 15206 412-665-3600	Feb 28, 2013 9:40 AM
4	Diana Haines Walton, Director Human Resources Management Division Metropolitan Police Department300 Indiana Avenue, NW, Room 6000 Washington, DC 20001 202 727 4261 diana.haines@dc.gov .	Feb 25, 2013 4:40 PM
5	Miriam Bryant, HR Coordinator, Virginia Beach PD, 757-385-4663, MBryant@vbgov.com	Feb 24, 2013 3:20 PM
6	Marty Humphrey Fort Worth Police Department marty.humphrey@fortworthtexas.gov (817) 392-4242	Feb 22, 2013 5:17 PM
7	Laura Adams, Administrative Specialist Montgomery County Police Department Personnel Division laura.adams@montgomerycountymd.gov 240-773-5312	Feb 22, 2013 2:10 PM
8	Lara Jones, Media Director Salt Lake City Police Department Desk: 801.799.3340 www.slcpd.com FB.com/slcpd Twitter.com/slcpd Youtube.com/saltlakecitypolice Pinterest.com/slcpd Instagram.com/slcpd MySpace.com/slcpolice Flickr.com/photos/slcpd	Feb 21, 2013 7:07 PM
9	Dwight L. Bower Fairfax County Police Department 571.641.6622 dwight.bower@fairfaxcounty.gov Note to MB and EL: please consider as invalid my responses to item 2, item 4, and item 11. In regard to item 11, discipline has been imposed based upon infractions of established policies, and social media utilization has been anecdotally an issue in some cases, but discipline is not imposed in specific regard to the social medial issues absent an approved social media policy.	Feb 21, 2013 6:36 PM
10	Alice Villagomez San Francisco Police Department (415) 553-1295	Feb 21, 2013 3:27 PM
11	Frank Domizio Philadelphia Police Department 215-669-5537	Feb 21, 2013 2:40 PM
12	Alan Bluemke Honolulu Police Department abluemke@honolulu.gov 808 723-3557	Feb 20, 2013 4:00 PM
13	n/a	Feb 20, 2013 1:05 PM
14	Daniel Hickson Metropolitan Police Department, Washington DC daniel.hickson@dc.gov 202-729-2035	Feb 19, 2013 7:20 PM
15	Deputy Director Regina Woolfolk PIO Jodie Silva Senior Police Officer Mike McCoy Houston Police Department 1200 Travis St. Houston, Texas 77002 regina.woolfolk@houstonpolice.org 713-308-3200	Feb 19, 2013 9:58 AM
16	Kenneth W. Lack Inspector Commanding Officer Public Information Office Nassau County Police Department 1490 Franklin Ave Mineola N.Y. 11501 Work 516-573-7135 Fax 516-573-7118 Klack@pdcn.org	Feb 14, 2013 12:28 PM

Page 1, Q20. Please provide contact information (name, department, email and phone number).

	www.police.nassaucountyny.gov	
17	Jill Celaya; Phoenix Police; jill.celaya@phoenix.gov	Feb 14, 2013 10:48 AM
18	Andrew Solberg 202-698-0111	Feb 12, 2013 7:09 PM
19	Cassandra Deck-Brown Raleigh Police Department 919 – 996-3385 Cassandra.Deck-Brown@raleighnc.gov	Feb 11, 2013 8:21 PM

APPENDIX II

Share Tweet

□

Yael Bar-tur / 1 day ago

Yael Bar-tur is a former communications liaison for the Israeli Military and graduate of the Harvard Kennedy School of Government. She has been an analyst for the New York City Police Department. Alejandro Alves also contributed to this article. They both write for presynched.com and tweet at @Yaelbt and @AlvesAA.

Those of us who spent the weekend simultaneously glued to televisions, police scanners and Twitter as the search for "Suspect #2" unfolded will walk away with some lessons in how information moves these days.

Disappointment in national media has become something of an Internet joke. But a serious consequence is the void in information that is both timely and reliable.

Into that void jumps the Internet public, hungry to consume and create information. The Reddit and 4chan army, unguided and without professional restraint, often contributed to the spread of rumors and misinformation. A single botched tweet and a misquote of a police scanner prompted swarms of Redditors to present Sunil Tripathi's head on a platter. While the community can and should take part in the effort to thwart criminals, an unguided mob will make unfortunate mistakes, which social media then amplifies.

Enter Boston Police and a commissioner who has long emphasized community relations.

Boston PD entered the conversation immediately because they knew chatter about the investigation would happen with or without them.

Commissioner Davis and Public Information Chief Cheryl Fiandaca, who headed up Boston PD's social media efforts, accomplished what no police department has done before: led conversation with citizens in a time of crisis.

They also listened, a step that is more remarkable than it sounds for many large organizations, let alone law enforcement. They used Twitter to track and correct the misinformation that media outlets spread.

SEE ALSO: It's Time for Truth on Social Media

The department’s tweet clarifying that there was no arrest shortly after the bombings saw more than 11,000 retweets. A polite scolding to those tweeting information from police scanners was retweeted more than 20,000 times, higher than any other tweet at that time and indication that the public accepts the fact that they too need to show some restraint.

By the end of the dramatic affair even the media was on board, as local reporters waited on a Boston Police tweet before officially announcing the capture of the elusive suspect.

Tweeting Isn't New for Boston Police

But that genuine engagement between police and citizens did not arise spontaneously after Monday morning’s explosions. Like any good relationship, the love affair between the police and the people of Boston built up slowly and took a lot of effort. Even before the BPD's follower count spiked this week, from 40,000 to more than 300,000, the department boasted more Twitter followers than most of the area’s local media.

True engagement does not arise in a time of crisis, but through preparation well ahead of the crisis.

Police leadership in Boston thought about how to directly incorporate social media into a broader mission of promoting safety, reducing fear and connecting with the community.

Last year when Anonymous downed the department's homepage, Commissioner Davis took to YouTube with a satirical video making light of the situation and assuring the public that several other channels of communication were still up and running. The department also established a "Tweet From the Beat" initiative.

Engagement will endure beyond the Boston Bombings because Boston PD gave the online community timely information and a sense of trust and familiarity. As the community conversations move from the coffee shops and the parks to the Twitter feeds and the chat rooms, BPD's presence online helps reinvent the whole notion of community policing for the 21st century.

SEE ALSO: Boston Bombings: Truth, Justice and the Wild West of Social Media

In an age where many people don’t necessarily trust their police force, this ongoing line of communication reminds us that, at the end of the day, officers are human beings (just ask Kevin “In-N-Out Real Quick” Brennan).

What's Next for @Boston_Police?

As we return to our daily routines and our fascination fades, BPD’s work — both on and offline — is just beginning. The huge spike in followers offers an opportunity to go one step further in police-community relations, and we can only hope that the BPD rolls out new social media initiatives.

A first step would be to take the commissioner’s “Tweet From the Beat” to the public and offer a few well-known Boston social media types a chance to ride along with the forces and broadcast their commentary. It may also be the time for the commissioner to hold town hall meetings online.

Commissioner Davis should also host an "Ask Me Anything" on Reddit. Such an unusual step of a public uniformed figure into the Internet's playground will help both sides built trust, not to mention allow them to learn a lot from each other, for next time.

These types of social initiatives will help prolong BPD’s moment in the sun, which unfortunately is not guaranteed to last forever.

Image via Jared Wickerham/Getty Images

TOPICS: BOSTON, BOSTON MARATHON, BOSTON POLICE, CRIME, SOCIAL MEDIA, TWITTER, U.S.

APPENDIX III

Global Justice Information Sharing Initiative

Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities

Guidance and Recommendations

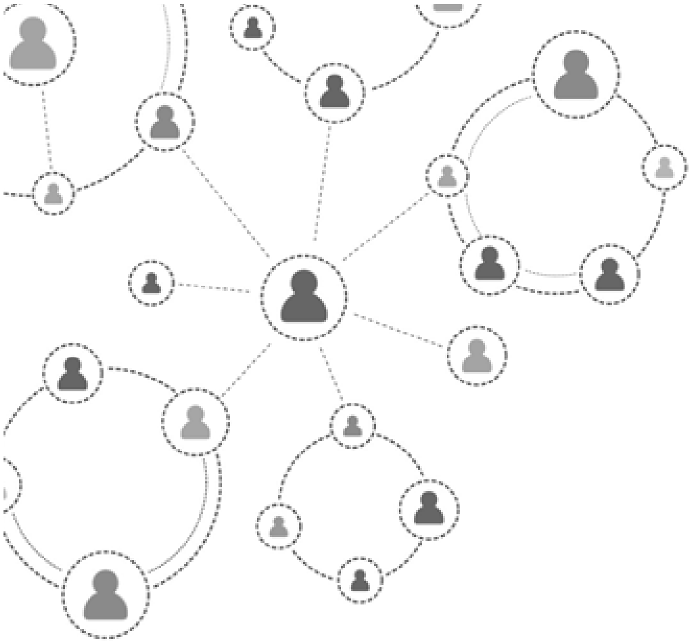
February 2013

Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities

Guidance and Recommendations

Table of Contents

This project was supported by Grant No. 2010-MU-BX-K019 awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, in collaboration with the Global Justice Information Sharing Initiative. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Justice.



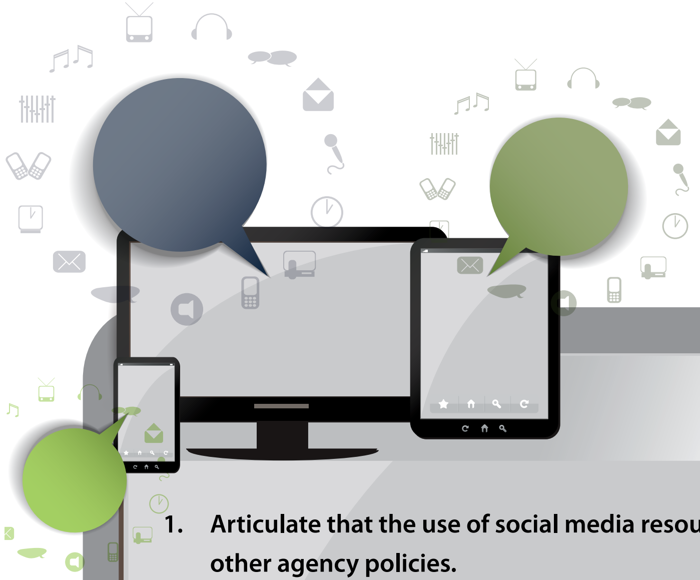
Executive Summary

The advent of social media sites has created an environment of greater connection among people, businesses, and organizations, serving as a useful tool to keep in touch and interact with one another. These sites enable increased information sharing at a more rapid pace, building and enhancing relationships and helping friends, coworkers, and families to stay connected. Persons or groups can instantaneously share photos or videos, coordinate events, and/or provide updates that are of interest to their friends, family, or customer base. Social media sites can also serve as a platform to enable persons and groups to express their First Amendment rights, including their political ideals, religious beliefs, or views on government and government agencies. Many government entities, including law enforcement agencies, are also using social media sites as a tool to interact with the public, such as posting information on crime trends, updating citizens on community events, or providing tips on keeping citizens safe.

Social media sites are increasingly being used to instigate or conduct criminal activity, and law enforcement personnel should understand the concept and function of these sites, as well as know how social media tools and resources can be used to prevent, mitigate, respond to, and investigate criminal activity.

Social media sites have become useful tools for the public and law enforcement entities, but criminals are also using these sites for wrongful purposes. Social media sites may be used to coordinate a criminal-related flash mob or plan a robbery, or terrorist groups may use social media sites to recruit new members and espouse their criminal intentions. Social media sites are increasingly being used to instigate or conduct criminal activity, and law enforcement personnel should understand the concept and function of these sites, as well as know how social media tools and resources can be used to prevent, mitigate, respond to, and investigate criminal activity. To ensure that information obtained from social media sites for investigative and criminal intelligence-related activity is used lawfully while also ensuring that individuals' and groups' privacy, civil rights, and civil liberties are protected, law enforcement agencies should have a social media policy (or include the use of social media sites in other information-related policies). This social media policy should communicate how information from social media sites can be utilized by law enforcement, as well as the differing levels of engagement—such as apparent/overt, discrete, or covert—with subjects when law enforcement personnel access social media sites, in addition to specifying the authorization requirements, if any, associated with each level of engagement. These levels of engagement may range from law enforcement personnel "viewing" information that is publicly available on social media sites to the creation of an undercover profile to directly interact with an identified criminal subject online. Articulating the agency's levels of engagement and authorization requirements is critical to agency personnel's understanding of how information from social media sites can be used by law enforcement and is a key aspect of a social media policy.

Social media sites and resources should be viewed as another tool in the law enforcement investigative toolbox and should be used in a manner that adheres to the same principles that govern all law enforcement activity, such as actions must be lawful and personnel must have a defined objective and a valid law enforcement purpose for gathering, maintaining, or sharing personally identifiable information (PII). In addition, any law enforcement action involving undercover activity (including developing an undercover profile on a social media site) should address supervisory approval, required documentation of activity, periodic reviews of activity, and the audit of undercover processes and behavior. Law enforcement agencies should also not collect or maintain the political, religious, or social views, associations, or activities of any individual or group, association, corporation, business, partnership, or organization unless there is a legitimate public safety purpose. These aforementioned principles help define and place limitations on law enforcement actions and ensure that individuals' and groups' privacy, civil rights, and civil liberties are diligently protected. When law enforcement personnel adhere to these principles, they are ensuring that their actions are performed with the highest respect for the



A Social Media Policy Should Address These Key Elements

1. **Articulate that the use of social media resources will be consistent with applicable laws, regulations, and other agency policies.**
2. **Define if and when the use of social media sites or tools is authorized (as well as use of information on these sites pursuant to the agency's legal authorities and mission requirements).**
3. **Articulate and define the authorization levels needed to use information from social media sites.**
4. **Specify that information obtained from social media resources will undergo evaluation to determine confidence levels (source reliability and content validity).**
5. **Specify the documentation, storage, and retention requirements related to information obtained from social media resources.**
6. **Identify the reasons and purpose, if any, for off-duty personnel to use social media information in connection with their law enforcement responsibilities, as well as how and when personal equipment may be utilized for an authorized law enforcement purpose.**
7. **Identify dissemination procedures for criminal intelligence and investigative products that contain information obtained from social media sites, including appropriate limitations on the dissemination of personally identifiable information.**

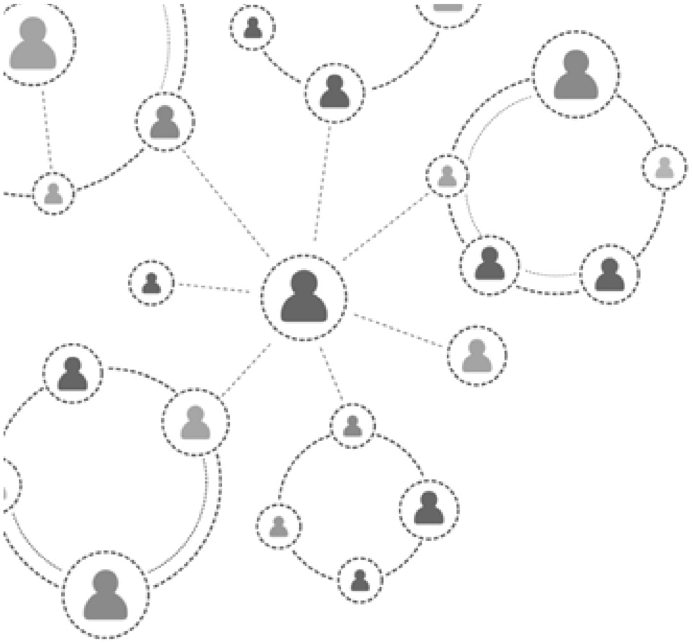
law and the community they serve, consequently fostering the community's trust in and support for law enforcement action.

The Bureau of Justice Assistance (BJA)—with the support of the Global Justice Information Sharing Initiative (Global) Advisory Committee (GAC), a Federal Advisory Committee (FAC) to the U.S. Attorney General on justice-related information sharing, and the Criminal Intelligence Coordinating Council (CICC)—has developed the resource *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations,* which provides law enforcement leadership and policymakers with recommendations and issues to consider when developing policy related to the use of social media information for criminal intelligence and investigative activities. A social media-related policy (or a policy that includes procedures on the use of social media information) will help protect the law enforcement agency and agency personnel and will also help ensure the continued protection of privacy, civil rights, and civil liberties of individuals and groups in the community.

The *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations* is designed to guide law enforcement agency personnel through the development of a social media policy by identifying elements that should be considered when drafting a policy, as well as issues to consider when developing a policy, focusing on privacy, civil rights, and civil liberties protections. This resource can also be used to modify and enhance existing policies to include social media information. All law enforcement agencies, regardless of size and jurisdiction, can benefit from the guidance identified in this resource.

The key elements identified in this resource can be applied to "traditional" social media sites (such as Facebook, Twitter, and YouTube) and are also applicable as different and new types of social media sites emerge and proliferate. As a policy is developed, the agency privacy officer and/or legal counsel should be consulted and involved in the process. Additionally, many agencies have an existing privacy policy that includes details on how to safeguard privacy, civil rights, and civil liberties, and an agency's social media-related policy should also communicate how these protections will be upheld when using information obtained from social media sites.

Social media sites have emerged as a method for instantaneous connection among people and groups; information obtained from these sites can also be a valuable resource for law enforcement in the prevention, identification, investigation, and prosecution of crimes. To that end, law enforcement leadership should ensure that their agency has a social media policy that outlines the associated procedures regarding the use of social media-related information in investigative and criminal intelligence activities, while articulating the importance of privacy, civil rights, and civil liberties protections. Moreover, the same procedures and prohibitions placed on law enforcement officers when patrolling the community or conducting an investigation should be in place when agency personnel are accessing, viewing, collecting, using, storing, retaining, and disseminating information obtained from social media sites. As these sites increase in popularity and usefulness, a social media policy is vital to ensuring that information from social media used in criminal intelligence and investigative activities is lawfully used, while also ensuring that individuals' and groups' privacy, civil rights, and civil liberties are diligently protected.



Introduction

In recent years, social media sites[1] have emerged as a useful tool for friends, coworkers, and families to keep in touch and interact with one another. Persons and groups can share photos or videos, coordinate meet-ups or plans for the weekend, and/or provide updates on newsworthy events to their friends, family, or customer base. One of the goals of these types of sites is instantaneous connections among people, businesses, and organizations, leading to greater and quicker sharing of information and enhanced relationships. Social media sites can also serve as a platform to enable people to express their First Amendment rights, including their political ideals, religious beliefs, or disappointments with government agencies. Many government entities, including law enforcement agencies, are now using social media sites to interact with the public and provide information on crime trends and community events and tips for keeping citizens safe.

To successfully and lawfully harness the power and value of social media sites, while ensuring that individuals' and groups' privacy, civil rights, and civil liberties are protected, agency leadership should support the development of a policy within their agency regarding the use of social media sites in criminal intelligence and investigative activity.

In addition to these types of information sharing exchanges between and among persons and entities, social media sites have become a tool that criminals are using for nefarious and criminal purposes. Examples of the use of social media to conduct criminal activity include individuals coordinating a criminal-related flash mob[2] or utilizing a social media site to plan a robbery, online predators joining a social media site to identify and interact with potential victims, and terrorist groups using social media to recruit new members and espouse criminal intentions. Because social media sites are increasingly being used to instigate and conduct criminal activity, law enforcement personnel should understand the concept and function of social media sites and know how social media tools and resources can be used to prevent, mitigate, respond to, and investigate criminal activity.

[1] The International Association of Chiefs of Police's (IACP) Center for Social Media defines *social media* as "a category of Internet-based resources that integrate user-generated content and user participation. This includes, but is not limited to, social networking sites (Facebook, MySpace), microblogging sites (Twitter), photo- and video-sharing sites (Flickr, YouTube), wikis (Wikipedia), blogs, and news sites (Digg, Reddit)."

[2] A *flash mob* is a "group of people, usually organized through social media or text message, that gather at a location to perform a specific action before dispersing. These actions may be for entertainment or criminal purposes." (http://www.IACPsocialmedia.org/glossary)

Social media sites can be valuable sources of information for law enforcement personnel as they fulfill their public safety mission—agency public information officers may use social media to interact with the public, detectives may access social media sites to assist in the identification and apprehension of criminal subjects, intelligence analysts may utilize social media resources as they develop intelligence products regarding emerging criminal activity, and fusion center analysts may use social media resources to assist in the development of analytic assessments. To successfully and lawfully harness the power and value of social media sites, while ensuring that individuals' and groups' privacy, civil rights, and civil liberties are protected, agency leadership should support the development of a policy within their agency regarding the use of social media sites in criminal intelligence and investigative activity.[3]

To assist agencies in drafting a social media policy, the Bureau of Justice Assistance (BJA)—with the support of the Global Justice Information Sharing Initiative (Global) Advisory Committee (GAC), a Federal Advisory Committee (FAC) to the U.S. Attorney General on justice-related information sharing, and the Criminal Intelligence Coordinating Council (CICC)—has developed this resource to provide law enforcement leadership and policymakers with recommendations and issues to consider related to the use of information obtained from social media sites as a part of criminal intelligence and investigative activities.[4]

It is recommended that all law enforcement leadership support the development of a social media-related policy and associated procedures (or enhance existing policies) to guide personnel on accessing, viewing, collecting, storing, retaining, and disseminating (or using) information from social media sites, tools, and resources as a part of their authorized investigative and criminal intelligence activities.[5] A written policy assists in the protection of the agency and agency personnel, as well as the individuals and groups in the community. With the advent of the Internet and, specifically, social media sites, the expectation of privacy has changed. Individuals and groups regularly make openly available various pieces of information of themselves (e.g., photos, relationship links, current locations, dates of birth); while in many cases this information is public and available to anyone with Internet access, law enforcement personnel should use this type of information only based upon a valid law enforcement purpose (i.e., consistent with legal authorities and mission requirements). A policy will assist agency personnel in identifying and understanding their purpose and limitations regarding the use of information from social media sites, the need to document this purpose, and the importance of protecting the public from inadvertent or intentional misuse of information obtained from social media sites.

This resource is designed to identify elements that should be considered for inclusion in a social media policy, issues to consider when developing a policy, and examples of the use of social media as an investigative or intelligence-related tool, focusing on the protection of privacy, civil rights, and civil liberties of individuals and groups. The tenets identified in this resource can be used to draft a new policy or enhance existing information and criminal intelligence-related policies.

[3] Agency leadership may also incorporate the tenets identified in the paper into existing policies and procedures (such as policies on criminal intelligence and/or criminal investigations).

[4] For purposes of this resource, *law enforcement* may be broadly defined to include all activities related to crime prevention or reduction and the enforcement of the criminal law. However, it is important to note that certain law enforcement or criminal justice agencies may be subject to additional constraints regarding access, use, or disclosure of social media sites and information. For example, prosecutors' offices must adhere to constitutional and statutory discovery and ethical standards that would not apply to police agencies. Consequently, nonpolice law enforcement agencies (such as state attorneys' offices or other prosecutorial entities) will need to take any unique considerations into account in developing a social media policy.

[5] For the purpose of this document, accessing, viewing, collecting, storing, retaining, and disseminating information obtained from social media sites, tools, and resources will be referred to as using information obtained from social media sites, tools, and resources.

Audience

All law enforcement agencies, regardless of size—from a small, rural agency to a large, metropolitan law enforcement agency to a state or urban area fusion center—can benefit from the recommendations identified in this document. As agency policymakers review the components of this resource, it should be understood that social media is, in essence, simply another resource for law enforcement personnel to use in the performance of their public safety mission. The same basic policing principles apply in the use of social media as with other law enforcement action.[6] It is important to provide all agency personnel—from leadership to analysts to detectives and investigators to uniformed patrol officers—with pertinent and applicable guidance to ensure that social media resources are being utilized in a lawful and appropriate manner, a manner that upholds the agency's mission and legal authorities and complies with applicable federal, state, and tribal laws and local ordinances. As agencies develop and adapt a policy on using social media information as a part of their investigative and intelligence-related activities (or enhance existing policies), it is recommended that the agency privacy officer and/or legal counsel be consulted and be involved in the development and implementation process.

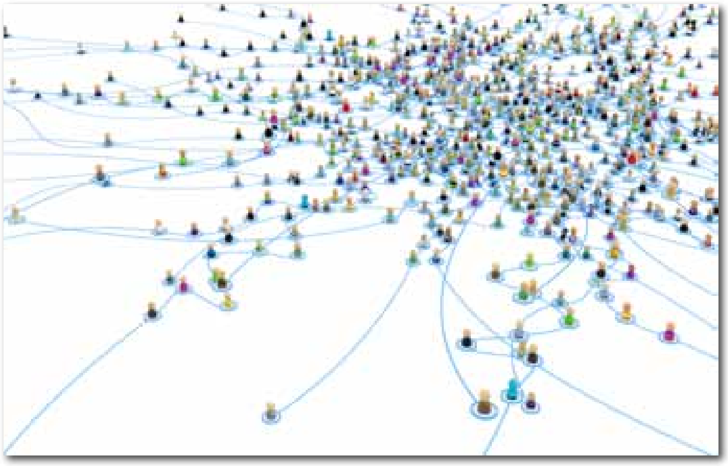
The Protection of Privacy, Civil Rights, and Civil Liberties

As with all law enforcement activity and actions, individuals' privacy, civil rights, and civil liberties must be diligently protected, and the proliferation of social media sites and technology has led to a renewed focus on these protections. Social media resources not only provide a new forum and format for free speech but also introduce a potential risk to individuals' privacy, civil rights, and civil liberties if unauthorized or inappropriate access or use occurs. To mitigate such risks, law enforcement officers and agency personnel are trained to ensure the protection of these rights while performing their duties, be it providing security at a public rally, conducting a criminal investigation, or developing criminal intelligence.[7] This type of training may also be applicable to the use of social media sites in investigative and intelligence activities and the privacy, civil rights, and civil liberties implications associated with access to social media sites and the use of information obtained from such sites.

In addition to training, many agencies have a privacy policy that includes details on how to protect individuals' and groups' privacy, civil rights, and civil liberties.[8] To support and enhance the agency's privacy policy, agencies should also have a policy regarding social media (or enhance existing information and criminal intelligence-related policies) that articulates how these protections will be upheld when using information obtained from social media sites and resources.

[6] See the section titled "Law Enforcement Principles" for additional information on these principles.
[7] An example of privacy training for line officers is available at http://www.ncirc.gov/training_privacylineofficer.cfm.
[8] Additional information on how to develop a privacy policy is available at http://www.it.ojp.gov/privacy.

Uses of Social Media



Social media may be used by law enforcement personnel in their daily functions in a number of areas, including:

- Pre-employment background investigations
- Outreach and community engagement
- Emergency alerts and notifications
- Analytic assessments
- Situational awareness reports
- Intelligence development
- Criminal investigations

Additional guidance for law enforcement agencies and personnel regarding pre-employment background investigations, outreach and community engagement, and emergency alerts and notifications is accessible via the International Association of Chiefs of Police's (IACP) Center for Social Media Web site, http://www.IACPsocialmedia.org/.

Analytic assessments and situational awareness reports can be designed to provide information to law enforcement on a specific topic to assist agencies in maintaining public safety. These assessments may serve as a gauge for determining the types of criminal activity within a region or determining whether there are threats related to an upcoming public event.[9] Information from social media sites may be referenced in an analytic assessment that identifies current levels of criminal activity within an agency's jurisdiction. For example, an agency may search Twitter feeds, which may contain information on gang-related activities, and Flickr, which may include pictures of gang-related graffiti. This information may then be referenced in an assessment to provide examples of the types of gang activity occurring within a certain area.

As it relates to criminal intelligence development and criminal investigations, information from social media sites may be used as a part of criminal-related background investigative activities. For example, a criminal subject's Facebook page may be accessed to further support the identification of the subject and/or acquaintances. Social media sites and resources may also be used to determine a timeline of events for a suspect. For example, when a person "checks in" on the Web site FourSquare at a certain date and time, this information may be accessible by Facebook users. The individual may then post a picture of himself at this location, which may also be geotagged[10] via a smartphone and uploaded by the individual to Twitter.

There are an ever-increasing number and variety of social media sites: simple Web sites to post short pieces of information, virtual worlds (e.g., Club Penguin, Second Life, massively multiplayer online role-playing games, or online gambling sites), photo-sharing sites, and online forums and comment areas. Although this document will focus on "traditional" social media sites while acknowledging the continuing emergence and proliferation of different types of social media, it should be understood that the elements set forth in this paper may be applied to all types of social media sites and resources.

[9] Additional information on responding to First Amendment-protected events is found in the *Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies*, available at http://it.ojp.gov/documents/First_Amendment_Guidance.pdf.

[10] The terms *geolocation/geotagging*, defined at www.IACPsocialmedia.org/glossary, refer to the incorporation of location data in various media, such as, for instance, a photograph, a video, or an SMS message. This may be used on social media platforms to notify people where a user is at a given time.

Elements of a Social Media Policy

The purpose of a social media policy is to define and articulate acceptable law enforcement practices related to using information obtained from social media sites. As a part of a social media policy, agency leadership should reference other related policies and/or general orders regarding both criminal intelligence and criminal investigations, including an agency's privacy policy or policy regarding undercover activities. Because social media sites can be used to support these functions, it is important to ensure consistency and continuity between policies or orders.

Key elements of a social media policy include:

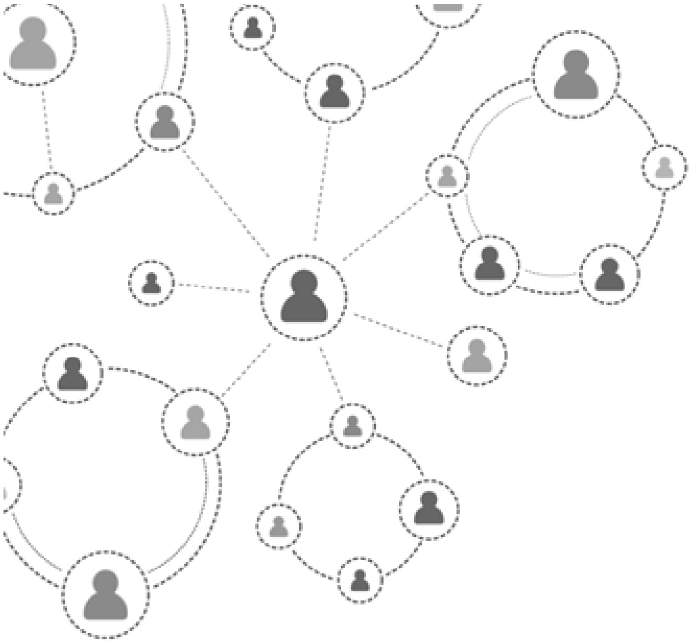
1. Articulate that the use of social media resources will be consistent with applicable laws, regulations, and other agency policies.
2. Define if and when the use of social media sites or tools is authorized (as well as use of information on these sites pursuant to the agency's legal authorities and mission requirements).
3. Articulate and define the authorization levels needed to use information from social media sites.
4. Specify that information obtained from social media resources will undergo evaluation to determine confidence levels (source reliability and content validity).
5. Specify the documentation, storage, and retention requirements related to information obtained from social media resources.
6. Identify the reasons and purpose, if any, for off-duty personnel to use social media information in connection with their law enforcement responsibilities, as well as how and when personal equipment may be utilized for an authorized law enforcement purpose.
7. Identify dissemination procedures for criminal intelligence and investigative products that contain information obtained from social media sites, including appropriate limitations on the dissemination of personally identifiable information (PII).

Law Enforcement Principles

Interwoven within these policy elements is the acknowledgement that social media sites and resources are another tool in law enforcement's toolbox of information sources. As such, social media sites and resources should be utilized in a manner that adheres to the same principles that govern all law enforcement actions. These principles include:

- Law enforcement actions must be lawful.
- Law enforcement actions should confirm with community standards, when appropriate.
- Law enforcement actions must have a defined objective and a valid law enforcement purpose for gathering, maintaining, or sharing personally identifiable information about criminal subjects.
- Law enforcement agencies should not collect or maintain information about the political, religious, or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless there is a legitimate public safety purpose, such as the information directly relates to criminal conduct or activity. In the case of criminal intelligence, such information should not be collected or maintained unless there is reasonable suspicion to believe that the subject of the information is or may be involved in criminal conduct or activity and the information is directly related to the criminal conduct or activity.
- Law enforcement policy directives must define:
  - » The circumstances under which conduct by personnel is authorized.
  - » The limitations on conduct by personnel.
- All law enforcement officers and support personnel must be properly trained.
- If law enforcement action involves undercover activity, the following areas should be addressed:
  - » Supervisory approval.
  - » Required documentation of activity.
  - » Periodic reviews of activity.
  - » Audit of undercover processes and behavior, including authorization time frames for undercover activities.

Regardless of the tools law enforcement personnel use to perform their duties, these principles help define and place limitations on actions undertaken by personnel and ensure the protection of individuals' and groups' privacy, civil rights, and civil liberties. The implementation of these principles will help ensure that all law enforcement action is performed with the highest respect for the law and for the community and will also help enhance the community's trust in law enforcement.



Social Media Policy Elements

Element 1 Articulate that the use of social media resources will be consistent with applicable laws, regulations, and other agency policies.

Background: Social media should be viewed as another tool in the law enforcement toolbox and should be subject to the same policies and guiding principles as other investigative methods and tools, including the identification of reasonable suspicion, a criminal predicate, or a criminal nexus and adherence to the agency's legal authorities and mission requirements.

Action: As a part of the agency's authorized law enforcement purpose, social media sites may be accessed to follow up on tips and leads, suspicious activity reports, investigative support, development of criminal intelligence, and the development of situational awareness reports. An agency policy on the use of social media resources as a part of investigative and intelligence-related activities should be similar to agency policies regarding the use of other investigative tools, such as undercover activities or accessing other types of open source information (e.g., Accurint or Internet-based search engines). Further, the social media policy should specify that personnel should be able to articulate the purpose of using information from social media sites, answering the questions "What are you using?" "Why are you using it?" "How did you use it?" and "Is there a time frame on its relevance?"

As a part of this continuity, a social media policy should specifically address:

- When the use of social media sites is authorized.
- The supervisory authorization process (if needed).
- Limitations on using information from social media sites.
- When and how social media sites may be accessed (e.g., during working hours or via agency resources).

Element 2

Define if and when the use of social media sites or tools is authorized (as well as use of information on these sites pursuant to the agency's legal authorities and mission requirements).

Background: Agency leadership and policymakers should be knowledgeable of applicable laws and regulations (including the U.S. Constitution; the Bill of Rights, specifically the Fourth Amendment; the state constitution; other laws; and 28 CFR Part 23) when developing a social media policy and should know how these laws affect using information obtained from social media sites.

Law enforcement has an obligation to comply with the Fourth Amendment. Every person has the right to be free from "unreasonable searches and seizures" of their "persons, houses, papers, and effects." These same protections may also apply towards the use of social media sites—the uploading of pictures, the posting of activities, and the relationships between and among individuals and groups. With the increasing use of technology and the free flow of information on the Internet, it may be difficult to discern what access is reasonable and what would be deemed unreasonable under the Fourth Amendment; therefore, a social media policy should clearly identify reasonable access to social media sites and the use of information obtained from social media sites.

In addition to the Fourth Amendment, the ***Katz*** test[11] establishes a method that can also be utilized as agency personnel analyze public or private information on social media sites. This test, based on ***Katz v. United States***, 389 U.S. 347 (1967), which addresses the expectation of privacy and intent to make information private, could also be applied to the use of social media information, specifically whether a social media site user has exhibited an expectation of privacy in the information and whether the expectation is one that society is ready to recognize as reasonable. For information posted on the Internet (via a social media site) that a user has made no effort to make private or conceal, applying the principles of the *Katz* test would most likely result in a determination that the information is public. However, law enforcement personnel should use that information only when there is an identified, valid law enforcement purpose.

28 CFR Part 23 may also assist agencies as they develop a social media policy. The 28 CFR Part 23 federal regulation has become the de facto national standard regarding criminal intelligence information systems. Although 28 CFR Part 23 regulates systems, many of its tenets may be applicable to a policy regarding social media, such as storage, retention, and sharing of information obtained from social media sites and resources. Additionally, 28 CFR Part 23 states that a project "shall not collect or maintain criminal intelligence information about the political, religious, or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity." This overarching purpose statement is also arguably pertinent to information obtained by law enforcement personnel via social media sites, specifically regarding what information personnel can store, retain, and disseminate on political, religious, or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization.

Action: A social media policy should articulate the parameters regarding using information obtained from social media sites. These parameters should be consistent with applicable laws, regulations, and other agency policies and further articulate how privacy, civil rights, and civil liberties protections are upheld during such activities. It is important to note that although information on many social media sites may be "open" (e.g., anyone with Internet access can view the information), ***law enforcement must be mindful of what is legal, as well as what is consistent with community standards and expectations, when using information from a social media site***. In other words, simply because information is

[11] See Appendix A for additional information on the ***Katz*** test and decision.

available to law enforcement does not mean it should be used by law enforcement in the absence of a clearly defined and valid law enforcement purpose. For example, a law enforcement investigator should search for and access an individual's Facebook profile when an authorized law enforcement purpose is identified, such as a search for a missing person or further identification of an alleged criminal, and not to look for information on a new neighbor.

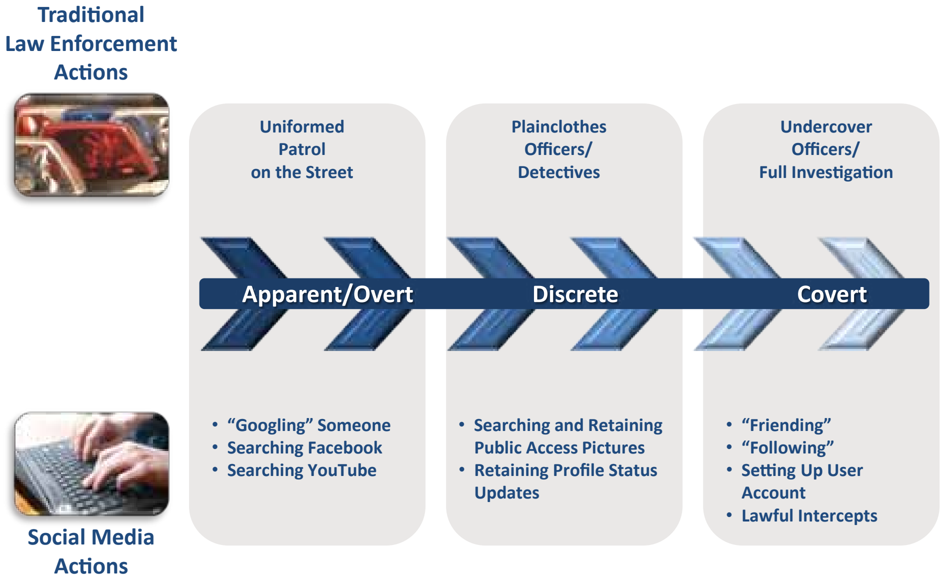
Relevant investigative laws, regulations, and policies should also be referenced in a social media policy. Articulating laws, regulations, and policies, as they relate to the use of social media sites and information, will support the agency and personnel in ensuring that they are using social media for a valid law enforcement purpose, adhering to established law enforcement principles, and protecting citizens' and groups' privacy, civil rights, and civil liberties.

Additionally, a social media policy (or policy that addresses information obtained from social media sites) should address the ever-changing nature of social media and associated technology. Technology advancements may affect the access and collection of information from social media sites, and a policy should acknowledge that though technology may change, the foundational elements for accessing social media sites remain consistent, such as accessing social media sites for an authorized law enforcement purpose.

Element 3

Articulate and define the authorization levels needed to use information from social media sites.

Background: Social media sites have varying and differing levels of access and engagement, ranging from "following" someone on Twitter to "friending" someone on Facebook or simply searching for an individual or a topic via Google. Engagement levels may also vary, from reviewing publicly available information on a social-networking site to accessing social media resources from a nongovernmental Internet Protocol (IP) address to creating a user profile or account for undercover operations to lawful intercepts of electronic information. Within the different engagement levels are privacy, civil rights, and civil liberties implications. A social media policy should articulate the levels of engagement by law enforcement personnel with subjects when accessing social media sites and also specify the authorization requirements associated with each level.


Traditional Law Enforcement Actions
Uniformed Patrol on the Street
Plainclothes Officers/ Detectives
Undercover Officers/ Full Investigation
Apparent/Overt
Discrete
Covert
• "Googling" Someone
• Searching Facebook
• Searching YouTube
• Searching and Retaining Public Access Pictures
• Retaining Profile Status Updates
• "Friending"
• "Following"
• Setting Up User Account
• Lawful Intercepts
Social Media Actions

As part of the levels of engagement, law enforcement personnel should understand privacy settings, end-user licensing agreements, and terms-of-service requirements. Users may regulate their privacy settings on their "profile," which in turn could affect the level-of-engagement parameters. Additionally, companies may articulate law enforcement engagement parameters via a terms-of-service agreement.[12]

[12] Many Internet- and communication-based companies have developed guides to assist law enforcement in understanding what information is available and how that information may be obtained. Additional information on these guides is available at the IACP's Center for Social Media, at http://www.IACPsocialmedia.org/investigativeguides.

To assist in understanding how information from social media sites can be used by law enforcement, the graphic above provides a visual demonstration of the comparison between traditional law enforcement practices and specific social media actions. As identified in the graphic, examples of levels of engagement include:

Apparent/Overt Use—In the Apparent/Overt Use engagement level, law enforcement's identification need not be concealed. Within this engagement level, there is no interaction between law enforcement personnel and the subject/group. This level of access is similar to an officer on patrol. Information accessed via this level is open to the public (anyone with Internet access can "see" the information). Law enforcement's use and response should be similar to how it uses and responds to information gathered during routine patrol. An example of Apparent/Overt Use would be agency personnel searching Twitter for any indication of a criminal-related flash mob to develop a situational awareness report for the jurisdiction.

Apparent/Overt Use is based on user profiles/user pages being "open"—in other words, anyone with Internet capabilities can access and view the user's information. For instance, if an officer searches for a criminal subject's Facebook page and determines that a profile which appears to be that of the subject has the account privacy settings set to "public" (meaning the information can be viewed by everyone), then the use of that information would be considered Apparent/Overt Use.

The authorization level for Apparent/Overt Use may be minimal, as this level of engagement is considered part of normal, authorized law enforcement activity (based on the law enforcement purpose).

Discrete Use—During the Discrete Use engagement level, law enforcement's identity is not overtly apparent. There is no direct interaction with subjects or groups; rather, activity at this level is focused on information and criminal intelligence gathering. The activities undertaken during the Discrete Use phase can be compared to the activities and purpose of an unmarked patrol car or a plainclothes police officer. An example of Discrete Use is an analyst utilizing a nongovernmental IP address to read a Weblog (or blog)[13] written by a known violent extremist who regularly makes threats against the government. Bloggers (those who write or oversee the writing of blogs) may use an analytical tool to track both "hits" to the blog and IP addresses of computers that access the blog, which could potentially identify law enforcement personnel to the blogger. This identification could negatively impact the use of the information and the safety of law enforcement personnel, who would not want to reveal that they are accessing the blog for authorized law enforcement purposes. In many cases, direct supervisory approval may not be necessary within this level of engagement, but the policy should address agency protocol.

Covert Use—During the Covert Use engagement level, law enforcement's identity is explicitly concealed. Law enforcement is engaging in authorized undercover activities for an articulated investigative purpose, and the concealment of the officer's identity is essential. An example of Covert Use is the creation of an undercover profile to directly interact with an identified criminal subject online. Another example is an agency lawfully intercepting infomation from a social media site, through a court order, as a part of authorized law enforcement action. Clear procedures should be identified and documented on the use of social media in this phase, since there are many privacy, civil rights, and civil liberties implications associated with Covert Use. Agencies should also review social media sites' information for law enforcement authorities and terms of service for additional information on undercover profiles.

Authorization levels for Covert Use activities should be clearly identified and could be compared to authorization levels needed for any undercover investigative activity (such as undercover narcotics investigations).

Action: An agency's social media policy should identify the agency's defined levels of engagement that will be utilized by agency personnel, the types of activity associated with these levels, and direct authorization requirements, if any,

[13] For additional information on blogs, please visit http://www.IACPsocialmedia.org/blogfactsheet.

associated with each level from use as a part of official law enforcement activities (e.g., the checking of social media sites is built into the analytic product development process) or direct supervisor approval requirements (such as development of an undercover profile to interact with a criminal subject). For example, if an agency uses social media to gather or disseminate information regarding a First Amendment-related event that has become violent in other jurisdictions, it is essential to clearly define any limits on the collection and use of information from social media.[14]

Element 4 Specify that information obtained from social media resources will undergo evaluation to determine confidence levels (source reliability and content validity).

Background: The evaluation of information—be it for criminal intelligence purposes or for criminal investigative purposes—may have differences. With regard to criminal intelligence, information should be assessed to determine its validity and reliability, and products produced as a result of this information should include proper caveats. In some instances, it may be difficult to determine the validity of information obtained from a social media site (e.g., a citizen submits a tip about a video posted on YouTube depicting a robbery); however, that information may still be considered a potentially valid tip and should be documented as such.

In the case of a criminal investigation, information obtained from a social media site should be further evaluated to ensure that the information is authentic. For example, a video posted on YouTube shows individuals allegedly robbing a convenience store; law enforcement personnel should obtain a subpoena to determine what IP address was used to upload the video and identify to whom the IP address is registered. Information obtained from social media sites can be a valuable tool; however, comprehensive evaluation and authentication are crucial to ensure the reliability and validity of the information and ensure proper caveats are included, as necessary.

Case law has recently been established regarding authentication of information obtained by law enforcement. In ***Griffin v. Maryland***, 2011 Md. LEXIS 226 (Md. 2011), the appeals court ruled that MySpace pages were erroneously admitted into evidence because they had not been properly authenticated. The trial court admitted the postings based on a police officer's testimony that the picture in the profile was of the purported owner and that they had the same location and date of birth. The picture, location, and birth date did not constitute sufficient "distinctive characteristics" to properly authenticate the MySpace printouts of the profile and posting because of the possibility that someone else could have made the profile or had access to it to make the posting. The court stated that there are different concerns when authenticating printouts from social media sites that go beyond the authentication concerns of e-mails, Internet chats, and text messages. Some suggested approaches to the social media authentication issue include an admission by the purported profile owner that it is his or her profile and he or she made the postings in question, a search of the person's computer and Internet history that links the subject to the profile or post, or information obtained directly from the social media site that identifies the person as the profile's owner and the individual with control over it, possibly including IP address identification information. This case demonstrates the need to validate information obtained from social media sites. ***As a source of information for lead development and follow-up, social media can be a valuable tool, but law enforcement personnel should always authenticate and validate any information captured from a social media Web site***.

Action: A social media policy should articulate that any information obtained from social media sites be evaluated to determine accuracy, validity, and/or authenticity. Social media interaction and usage are based on user uploads and updates and therefore should not serve as a primary/sole source for information gathering and verification. As with all sources of information, independent validation is important to determine accuracy and, more important, to protect individuals

[14] See *Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies* for additional information on law enforcement's role regarding First Amendment-protected events.

from being incorrectly identified, possibly leading to privacy violations and/or other inappropriate actions. Agencies may also refer to other policies and procedures related to criminal intelligence and investigative activities (and sources of information) as a part of the evaluation and authentication processes of information obtained from social media sites.

Element 5

Specify the documentation, storage, and retention requirements related to information obtained from social media resources.

Background: Based on the purpose for gathering information via social media resources (e.g., intelligence development, analysis assessment, or criminal investigations), agencies should identify the storage and retention requirements (why and for how long this type of information should be retained).[15] For criminal intelligence development and products, agencies may reference the storage and retention requirements identified in 28 CFR Part 23. For the documentation, storage, and retention requirements of information obtained from social media sites that is being utilized for a criminal investigation, agencies should refer to their investigative policies and procedures (and applicable laws and regulations).

If personally identifiable information (PII) (such as a name, a date of birth, or a picture) is identified and collected from social media sites, agencies should be sensitive to the documentation and retention of this information. If the information is part of criminal intelligence development, it is recommended that the tenets of 28 CFR Part 23 be followed; if the information is part of a criminal investigation, it is recommended that agency policy and procedures related to the dissemination of investigative information be referenced.

The documentation of this type of information should specify the purpose of the information use (regardless of the source of information), what information was collected (photos, status updates, friends), when the information was accessed and/or collected, where the information was accessed (identify the Web site), and how the information was collected (open search, nongovernmental IP address, undercover identity, etc.). Copies of the information obtained from the sites should also be documented. Additionally, as law enforcement personnel access social media sites, the reason for the use of the information obtained and the site utilized should be specified in the case or intelligence file.

For analysis assessments, the storage and retention period will be contingent on the assessment findings and whether a valid law enforcement purpose was identified. For example, a local law enforcement agency sends a request for information to the state fusion center to determine whether there are any threats or potential criminal activity associated with an upcoming demonstration. The fusion center creates an awareness assessment and references information obtained from social media resources that articulates that there are no threats identified. Further, the demonstration was peaceful, with no arrests. No potential criminal predicate or criminal nexus was identified either in the assessment itself or during the event, and therefore there is no articulable reason to store the information that was obtained as part of the analysis assessment.

For intelligence development purposes, the requirements of 28 CFR Part 23 should be followed regarding storage and retention of all information, whether collected from social media sites or other information sources. Though not all intelligence systems are required to adhere to 28 CFR Part 23, it has become a de facto national standard,[16] and as such, agencies are strongly encouraged to incorporate the tenets of this regulation into their policies and procedures regarding all criminal intelligence-related information.

[15] For additional information on file guidelines for criminal intelligence, please refer to the LEIU *Criminal Intelligence File Guidelines*, http://it.ojp.gov/documents/ncisp/criminal_intel_file_guidelines.pdf.

[16] See the *National Criminal Intelligence Sharing Plan*, Recommendation 9, http://it.ojp.gov/documents/NCISP_Plan.pdf.

If information from a social media site was gathered as part of a criminal investigation—such as a photo, identification of associates, or other PII—law enforcement personnel should adhere to agency policies and procedures regarding the documentation and storage of such information, carefully noting when and where the information was gathered.[17] A policy should also address the need to print or record the information gathered from the site to include in the case file for evidentiary purposes, due to the ease of changing social media information (users deleting information, changing their settings, etc.).

Action: The documentation, storage, and retention requirements for information obtained from social media resources should be articulated and defined in a social media policy. This section of the policy should be comparable to other investigative and/or intelligence policies regarding information documentation, storage, and retention.

Element 6

Identify the reasons and purpose, if any, for off-duty personnel to use social media information in connection with their law enforcement responsibilities, as well as how and when personal equipment may be utilized for an authorized law enforcement purpose.

Background: The ease and accessibility of social media resources (including the use of applications [or apps] for smartphones and tablet computers) may affect how law enforcement personnel access social media when off duty,[18] as well as the use of personal equipment and personal accounts for official agency purposes. The information that is collected may result in criminal intelligence or lead to an active investigation; therefore, it is important to include a provision in the social media policy to address using information from social media sites for a law enforcement purpose by off-duty personnel and using nonagency equipment for official law enforcement purposes. With greater access to information through social media sites, it may be easier to identify criminal subjects and/or criminal activity, but it is also imperative to identify approved uses and access to the information.

For example, a law enforcement officer is off duty and is posting an update on his Twitter page. As part of his accessing Twitter on his personal computer, he notices a trending topic for his city about a robbery at a jewelry store. The agency's social media policy might require that the officer report this issue to dispatch and conduct a follow-up field incident report, documenting what he viewed, the site where he viewed the information, when he viewed it, and any action based on the information. In another example, an analyst is viewing her friends' status updates on Google+ and notices one friend expressing outrage at recent government policies (the friend does not make any threats, just articulates dissatisfaction). This posting is part of her friend's First Amendment right to free speech, and therefore no law enforcement documentation or other action should take place.

In another example, an intelligence officer who is focused on gang-related crime uses his personal Twitter account to "follow" a subject-matter expert (SME) in the field of gang identification and trends, as authorized in the agency's policy, which includes the provision for law enforcement officers to access social media sites, via personal accounts, as a part of their authorized law enforcement mission. The officer regularly updates his supervisor and intelligence unit members of trends identified by the SME and how these trends may be carried out in the jurisdiction.

Because of the widespread use of social media, agency policy must articulate when and how it is acceptable for off-duty personnel to use information from social media sites as part of their law enforcement mission. Law enforcement personnel

[17] It is important to note that the gathering of information from a social media site may be the result of a court-ordered lawful intercept. As such, there may be specific instructions regarding the gathering and storage of information.

[18] The IACP's Center for Social Media identifies five key policy considerations for agency policies regarding the use of social media, including the use of social media for personal use. See http://www.iacpsocialmedia.org/GettingStarted/PolicyDevelopment.aspx.

must adhere to law enforcement principles, whether on duty or at home surfing the Internet for a law enforcement purpose.

Action: A policy that addresses social media information should specify whether or not off-duty personnel may, as a part of an authorized law enforcement purpose, access social media sites and the reason(s) (if any) and requirements for access. If authorized, the policy should address the parameters in regards to accessing information that is viewed and gathered by off-duty personnel (for an authorized purpose), restrictions on the use of work equipment and/or personal equipment in an official law enforcement capacity while off-duty, and how to document and report the information that is gathered from the social media site. [19]

The policy should also specify whether or not law enforcement personnel may, when carrying out their authorized law enforcement mission and function, use personal equipment (including personal accounts) to access information via social media sites and the reason(s) and requirements associated with the use of personal equipment for this purpose. If the policy indicates that it is acceptable to use personal equipment for official agency purposes, then the policy should also direct personnel to document how information was obtained, the type of information obtained, the reason the information was obtained, and any follow-up action.

Element 7 Identify dissemination procedures for criminal intelligence and investigative products that contain information obtained from social media sites, including appropriate limitations on the dissemination of personally identifiable information.

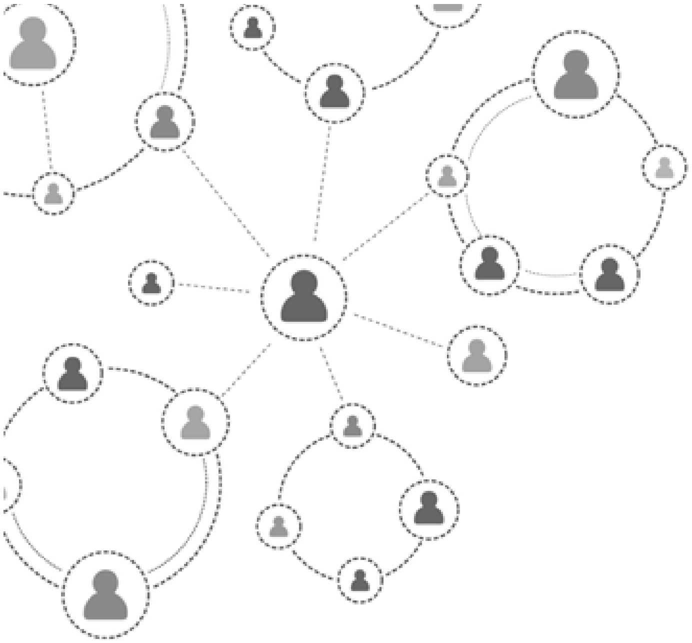
Background: Because of the open nature of many types of information obtained from social media sites, it is important to articulate dissemination procedures of products, reports, and requests for information that include information from social media sites.[20]

Additionally, the use of social media sites that focus on advocating greater information sharing among law enforcement agencies and personnel should be addressed in a policy. These sites offer greater access and information sharing capabilities; however, sharing any type of law enforcement information should be limited to nationally recognized sensitive but unclassified (SBU) networks (e.g., Regional Information Sharing Systems® [RISS], Law Enforcement Online [LEO], Homeland Security Information Network [HSIN]) and not social media/open source, commercially developed platforms.

Action: A social media policy should address dissemination protocols (who to disseminate to, timeline restrictions, how to disseminate information) for law enforcement reports, products, bulletins, and other types of information that may include information obtained from social media sites (and contain criminal intelligence information, criminal investigative information, and other information containing PII). Additionally, because of the sensitive nature of this type of information, the policy should address the incorporation of a review from a privacy officer and/or general counsel when disseminating products that include information from a social media site (including biographical information, photos, locations of subjects, etc.). A policy should also address dissemination mechanisms, such as using secure e-mail and SBU systems (not open source systems) to share criminal intelligence versus the use of social media sites to post bulletins to educate the public about criminal activity in the community.

[19] The IACP's Center for Social Media further addresses employee personal use of social media.

[20] For example, the validity and reliability of PII (e.g., photos, videos, and biographical information on a subject) that was obtained from social media sites may be unknown.

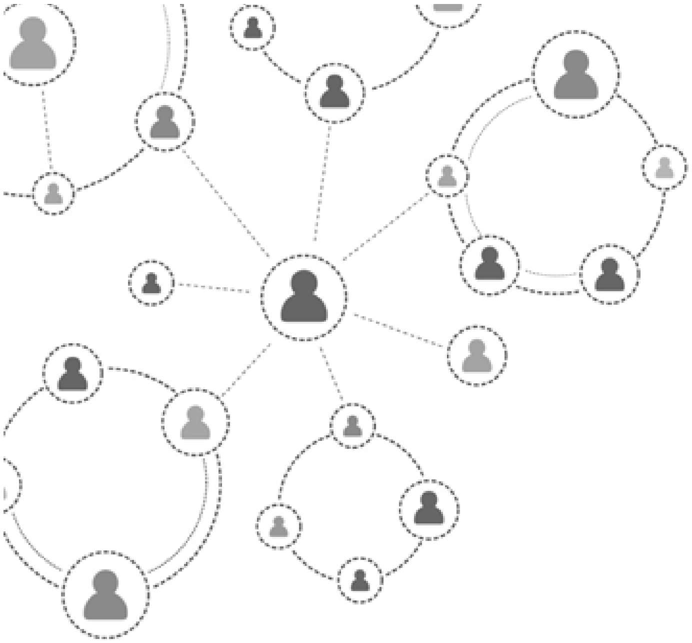


Conclusion

Social media sites and resources may be a helpful tool for law enforcement personnel in the prevention, identification, investigation, and prosecution of crimes. Though social media sites are a relatively new resource for law enforcement, the same principles that govern all law enforcement activities should be adhered to as personnel access, view, collect, use, store, retain, and disseminate information from these types of sites; the same procedures and prohibitions that are placed on law enforcement officers when patrolling the community or conducting an investigation should be in place when law enforcement personnel utilize social media as a part of their public safety function.

As with other law enforcement tools—such as uniform patrol, undercover activities, and search warrants—it is important to have a policy that articulates the how, when, and why of accessing, viewing, collecting, using, storing, and disseminating information obtained from social media sites, highlighting the privacy, civil rights, and civil liberties protections that are in place, regardless of the information source.

Though social media sites are a relatively new resource for law enforcement, the same principles that govern all law enforcement activities should be adhered to as personnel access, view, collect, use, store, retain, and disseminate information from these types of sites.



Appendix A—Cases and Authorities

These cases and authorities were relied on in the construction of the *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations* document. While these may be persuasive, it is always prudent to have agency legal counsel examine them in light of the controlling legal authorities in your jurisdiction.

Fourth Amendment Privacy Law and the Internet

Expectation of Privacy in Internet Communications, 92 A.L.R.5th 15, contains a good summary of current law regarding many forms of Internet communication, including e-mail messages and inboxes, chat rooms, Web site content, and social-networking sites. Many cases cited within are summarized below.

Smith v. Maryland, 442 U.S. 735 (1979), forms the basis of the "third-party exposure" doctrine of electronic privacy law. In *Smith*, the government used pen register technology to record the numbers dialed out from a certain phone number. This information was used to convict the defendant of robbery. The defendant challenged the use of the pen register as an illegal search under the Fourth Amendment. The court ruled that the defendant did not have a reasonable expectation of privacy in the phone record information because the information was automatically turned over to a third party, the phone company. Even if the defendant had an expectation of privacy in the numbers dialed, it was not one society recognized as reasonable—therefore, there was no Fourth Amendment violation. This case has been analogized to Internet subscriber information, such as account existence and information on who the registered user of the account is because this information is automatically exposed to a third party, the Internet service provider.

United States v. Jones, 132 S. Ct. 945 (2012), is a case involving law enforcement's placement of a Global Positioning System (GPS) device on a subject's car and use of the device to monitor the vehicle's movement on public streets for a four-week period (which extended beyond the period of time and place authorized by a search warrant). The Supreme Court Justices unanimously agreed that use of the GPS device constituted a search within the meaning of the Fourth Amendment. The majority explained that a physical intrusion into a constitutionally protected area, coupled with an attempt to obtain information, can constitute a violation of the Fourth Amendment based upon a theory of common law trespass. The majority explained that "the use of longer-term GPS monitoring in investigations of most offenses impinges on expectations of privacy." Additionally, in a separate opinion, one justice suggested that it may be time to rethink all police use of tracking technology, not just long-term GPS, reasoning that "GPS monitoring generates a precise, comprehensive record of a person's public movement that reflects a wealth of detail about her familial, political, religious, and sexual associations…. The government can store such records and efficiently mine them for years to come." The reasoning expressed by the justices in Jones could have broad implications for law enforcement use of social media in such areas as law enforcement personnel access to information from social media sites and the determination as to whether the social media user has a reasonable expectation of privacy due to privacy controls set up by the user.

United States v. Kennedy, 81 F. Supp. 2d 1103 (D. Kan. 2000). Relying on *Smith* (above), the District Court of Kansas ruled that the defendant did not have a reasonable expectation of privacy in information knowingly turned over to his Internet service provider, including Internet subscriber information and information associated with his Internet Protocol (IP) address. Divulgence of this information to law enforcement by Road Runner cable did not violate defendant's Fourth Amendment rights. See also ***United States v. Ohnesorge***, 60 M.J. 946 (N.M. Ct. Crim. App. 2005) (the court did not abuse its discretion in refusing to suppress Internet service provider information, specifically subscription information to a news and file access sharing Web site obtained without a warrant. The defendant did not have a reasonable expectation of privacy in the information; the subscription information was never confidential, and the defendant acknowledged that the information could be shared in the terms of service agreement with the site).

Social Media and Privacy Law

Nathan Petrashek Comment, "**The Fourth Amendment and the Brave New World of Online Social Networking**," 93 Marq. L. Rev. 1495 (summer 2010). This law review article provides a thorough background on social-networking sites and how the two largest, MySpace and Facebook, operate. A current case law summary is provided as well as an explanation of different privacy doctrines and how they can be applied to the social media setting.

Katz v. United States, 389 U.S. 347 (1967), provides the foundation for most federal court privacy rulings and doctrines. *Katz* moved away from previous Supreme Court privacy jurisprudence in holding that the Fourth Amendment protects people and not places, overruling the previous "trespass" doctrine of Fourth Amendment protection. Fourth Amendment considerations no longer require a physical invasion or trespass. In this case, police eavesdropped on private conversations from a public telephone booth, and the court found that even though no physical invasion of the phone booth occurred, this was not necessary to constitute a search for purposes of the Fourth Amendment. Police violated the defendant's Fourth Amendment privacy interests by listening to the content of the conversations without a proper warrant. *Katz* established a two-prong test to determine whether the Fourth Amendment is implicated and a search has occurred. If a person, like Katz, has manifested an intent to make the information private *and* society accepts that expectation of privacy as reasonable, then that privacy expectation cannot be violated without following Fourth Amendment warrant requirements.

Minnesota v. Olson, 495 U.S. 91 (1990), further explained the application of *Katz* and the two-prong expectation of privacy test. As an overnight guest, the defendant did have an expectation of privacy in the dwelling, and that expectation is recognized by society as reasonable.

Courtright v. Madigan, 2009 U.S. Dist. LEXIS 102544 (S.D. Ill. 2009). The defendant was convicted of three separate offenses of producing, possessing, and receipt of child pornography by a repeat offender. The case initiated through a subpoena served on MySpace.com by the Illinois Attorney General's Office in an effort to learn whether any registered sex offenders were using that site. Upon learning the defendant had a MySpace account, investigators took further steps to discover his IP address and learned that this address had offered pornographic images on the file-sharing site Limewire. These discoveries formed the basis of a warrant that uncovered evidence that was used to convict the defendant. The defendant argued that the initial information gathered from MySpace regarding his account violated his protection against unreasonable searches and seizures under the Fourth Amendment. For other procedural reasons, the defendant's appeal was denied, but the court addressed the search issue and, relying on multiple other courts, held that the defendant had no privacy expectation in Internet subscriber information based on the third-party exposure doctrine. The defendant had no expectation of privacy in the fact that his MySpace account existed, so the request for information on that matter did not violate his Fourth Amendment rights.

Commonwealth v. Proetto, 771 A.2d 823 (Pa. Super. Ct. 2001). In *Proetto*, the defendant was brought to the attention of police after a 15-year-old female who had been contacted by the defendant in a public chat room turned over logs of chats that contained explicit information and solicited sexual activity from the underage girl. Police asked the informant to cease communication with the defendant but inform them when he was online again. When police were informed that the defendant was online, they entered the chat room the defendant was in, posing as a 15-year-old girl. The defendant made sexually suggestive comments to the "underage female," which law enforcement officers logged. The defendant challenged use of the chat room logs and e-mail messages under the Fourth Amendment and Pennsylvania Wiretap Act. First, for the communication forwarded to police from the underage informant, the court analogized the e-mail and chat communications to letters and found a limited privacy right. As with letters, the expectation of privacy in the information was reasonable until the intended recipient received the information. After that, because the information could easily be forwarded to others, there remains no reasonable expectation of privacy; therefore, there was no Fourth Amendment violation. For the chats, the defendant did not know exactly whom he was speaking to so he did not have a reasonable expectation of privacy. Communications made directly to the undercover officer survive Fourth Amendment challenges under the same reasoning in that the defendant has only limited privacy interests in e-mail communications. Because the defendant communicated freely with the undercover officer and could not verify the officer's identity, he had no reasonable expectation of privacy in the chat communications. The fact that the officer did not identify himself as law enforcement is of no consequence. The Pennsylvania Wiretap Act was not violated because the informant and the police were both the intended recipients and parties to the communication and recorded the messages concurrently with the communication. For similar case law, see ***United States v. Maxwell***, 45 M.J. 406 (C.A.A.F. 1996) (no expectation of privacy found in e-mail communications in child pornography case); ***United States v. Charbonneau***, 979 F. Supp. 1177 (S.D. Ohio 1997) (explaining chat room and privacy expectations around Internet service providers, finding no reasonable expectation of privacy); and ***Ohio v. Turner***, 156 Ohio App. 3d 177 (Ohio Ct. App. 2004) (no expectation of privacy in chat room conversations with undercover agent posing as underage boy).

Guest v. Leis, 255 F.3d 325 (6th Cir. 2001). After receiving a tip regarding online obscenity, police began investigating two electronic bulletin board systems. Police assumed an undercover identity to receive a password to the bulletin board, which enabled them to send e-mails to members, post messages, and share pictures, among other things. After viewing pornographic activity, the police obtained subscriber information from the bulletin boards. Defendants filed a class-action suit citing violation of their Fourth Amendment rights when the police accessed subscriber information for the bulletin boards, which included the subscribers' name, address, birth date, and password. The court concluded that, like other information provided to a third party, this information was not protected by the Fourth Amendment and there is no reasonable expectation of privacy attached to it.

J.S. v. Bethlehem Area School District, 757 A.2d 412 (Pa. Commw. Ct. 2000), involved a student's off-campus Web site postings. A student created a Web site with derogatory comments about a teacher and the school administration. As a result of these postings, the student was expelled. The court found that the school did not violate the student's privacy rights when accessing the materials posted on the Web site. The Web site was not password-protected and was available to anyone that came across it on the Internet. The court reasoned that once material is published on a Web site, it is open to the public. If the creator does not take any steps to protect the Web site content and make it private, no expectation of privacy can be said to exist. See also ***Konop v. Hawaiian Airlines, Inc.***, 236 F.3d 1035 (9th Cir. 2001) (employer did not violate employee's privacy rights by accessing public, unprotected Web site postings. *Konop* held there is no expectation of privacy in information posted to public Web sites).

United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009). This case involved use of a fake MySpace profile that was created and used in violation of the Web site's terms of service contract agreed to by all users. The Central District of California's court found that in some instances, the violation of a terms of service agreement could constitute a misdemeanor offense under the Computer Fraud and Abuse Act. The court vacated the conviction, however, because the statute did not pass the constitutionality void for vagueness test based on the absence of guidelines in the statutory scheme to guide law enforcement and an actual notice requirement. Although involving civilian use of social media, the reasoning and analysis could be useful to guide law enforcement officers who are using social media and fake profiles in undercover investigations.

Documenting Social Media During an Investigation

Todd G. Shipley, ***Collecting Legally Defensible Online Evidence: Creating a Standard Framework for Internet Forensic Investigations***. Vere Software Investigative Tools. December 2001. Available at http://veresoftware.com/uploads/CollectingLegallyDefensibleOnlineEvidence.pdf. Last accessed June 9, 2011. This document explains the difference between Internet evidence gathering and traditional computer-based evidence gathering. The collection, preservation, and presentation technique for gathering Internet evidence is explained in the document. References to outside sources and summaries of some documentation techniques are also included.

Kyllo v. United States, 533 U.S. 27 (2001), establishes the Supreme Court rule on advanced technology use in searches. In *Kyllo*, the police suspected the defendant of growing marijuana inside his residence. They utilized thermal imaging equipment to "peer through" the walls of the home and determine the defendant was growing marijuana. The court of appeals upheld the search on the basis that the defendant did not make any effort to conceal the heat emanating from his home and therefore did not have a reasonable expectation of privacy under the Fourth Amendment. The Supreme Court reversed, holding that the thermal imaging infiltrated the home and did constitute a search under the Fourth Amendment. The Supreme Court ruled that it was a search in violation of the Fourth Amendment because the thermal imaging gained information, through technology not generally used by the public, that could not have otherwise been gained without physical intrusion of the home, a constitutionally protected area without a warrant.

Hubbard v. MySpace, Inc., 2011 U.S. Dist. LEXIS 58249 (S.D. N.Y. 2011), establishes that social-networking sites, such as MySpace, can provide account user information, IP address information, IP address use date and time logs, *and* contents of the user's private messages and sent-message folders to law enforcement in response to a valid subpoena or warrant under the Electronic Communications Privacy Act.

Authenticating Social Media Evidence

Authentication of Electronically Stored Evidence, Including Text Messages and E-Mail, 34 A.L.R.6th 253. This document outlines the state of case law regarding authentication of various electronic communications, including text messages, e-mails, chat and instant messages, and others. This source provides general background on authentication issues with electronically stored communications; however, the agency or office will need to check the jurisdiction's specific requirements.

Griffin v. Maryland, 2011 Md. LEXIS 226 (Md. 2011). In a case involving evidence of witness intimidation obtained from a MySpace profile purported to be that of the defendant's girlfriend, the court relied upon officer testimony. Based on the picture on the profile, the defendant's girlfriend's birthday and profile birthday being the same, and the location listed on the profile, it was determined that this was the profile of the defendant's girlfriend. The trial court authenticated the evidence solely on officer testimony regarding the profile's information and admitted it into evidence. On appeal, the court found error because no extrinsic evidence was used to authenticate the profile or posting. The court reasoned that the picture, location, and birth date alone are not sufficient "distinctive characteristics" to authenticate a MySpace profile printout because someone else could have created the page and made the posting.

Lorraine v. Markel American Insurance Company, 241 F.R.D. 534 (D. Md. 2007), outlines the various ways digital and Internet-based evidence can be authenticated in court. The opinion analyzes the applicable federal rules of evidence and how they can be applied to electronically stored evidence. The opinion provides a good guide for law enforcement with respect to the type of information needed for the authentication of Internet-based evidence. Specifically, the opinion explores identifying and authenticating characteristics of e-mail messages, Internet Web site postings, text messages and chat room content, computer-stored and -generated data, and digital photographs. Citations to cases in other jurisdictions explaining electronic evidence authentication are also included.

Successful Use of Social Media Evidence in Investigations and Trials

U.S. v. Underwood, 2010 U.S. Dist. LEXIS 134543 (W.D. Ky. 2010), is a case regarding child pornography and enticing a minor charges. The charges originated from an undercover police investigation conducted online with an officer posing as a 13-year-old boy. The investigation was initiated after an anonymous caller to the police tip line reported a possible pedophile operating on the MySpace social-networking Web site. The police officer then created an undercover profile purporting to be a 13-year-old boy and sent a friend request to the defendant. The defendant engaged the undercover officer in communication on the MySpace and Yahoo! Web sites, with much of the conversation having a sexual nature. Based on this initial investigation, subpoenas were served on the Web sites and various Internet service providers, which resulted in identification of the defendant as the various accounts' holder, the IP addresses associated with those accounts, and his home address. This was used to apply for a search warrant of the defendant's house. Evidence was suppressed because the warrant issued was for evidence of child pornography, while the affidavit accompanying the application referred only to the crime of enticing a minor. In this case, redaction of the warrant and partial suppression were not an adequate remedy; however, probable cause had been established by the social media evidence for a warrant to search for evidence of enticing a minor. If not for the discrepancy in the request to search for evidence and a warrant issued for child pornography crimes and the probable cause listed in the application for enticing a minor, the social media evidence would have provided valid probable cause to issue a warrant. See also ***U.S. v. Lee***, 603 F.3d 904 (11th Cir. 2010) (evidence from a social-networking site was sufficient to uphold convictions of attempted enticement of a minor, attempted production of child pornography, and knowing receipt of child pornography even though communications through the site were with an adult and the children were fictitious. Evidence consisted of multiple online conversations between an undercover postal inspector and the defendant and one recorded phone call); ***U.S. v. Schene***, 543 F.3d 627 (10th Cir. 2008) (social media investigation evidence and computer account activity used to confirm that the defendant was in fact the person at the IP address who received child pornography).

In the Interest of F.P., 878 A.2d 91 (Pa. Super. Ct. 2005), is a case involving a juvenile delinquency charge resulting from an assault. Evidence used to support a finding of delinquency included instant messages sent from the delinquent juvenile to the victim. The juvenile challenged their admission based on improper authentication because no evidence of their source from the Internet service provider or by a computer forensics expert was provided. The court upheld the finding of delinquency and ruled the authentication was proper based on the circumstantial evidence provided at the adjudication hearing. The basis for authenticating the instant messages rested on the facts that the juvenile identified himself with his first name in the conversations, made accusations in the conversations that were consistent with testimony of other witnesses, and referenced the victim reporting the threats to school officials. Moreover, the character of the messages and conversations was consistent with other testimony regarding the juvenile's feelings and actions towards the victim. These circumstantial facts were sufficient to authenticate the instant messages as coming from the delinquent juvenile.

A.B. v. Indiana, 885 N.E. 2d 1223 (Ind. 2008), involves alleged threats made by a student against her principal on the MySpace social-networking site. The opinion does not address authentication issues but does provide an overview on how the MySpace site functions and explains the difference between "public" and "private" profiles, groups, and postings. Authentication issues were resolved by student testimony and permission to access the MySpace postings from their profile, which was "friends" with the appellant student's admitted profile.

Munoz v. State, 2009 Tex. App. LEXIS 256 (Tex. App. 2009). The defendant challenged, among other things, a criminal street gang enhancement charge. During the course of an assault trial resulting from a drive-by shooting incident, an investigator with the district attorney's office testified as to how to identify gang members and that based on his investigation, the defendant was a gang member. Several MySpace pictures the investigator used to form his opinion on gang involvement were admitted into evidence. The investigator, who maintained a local gang database and was knowledgeable on local gang activity, provided testimony and evidence from his MySpace investigations of the defendant. This testimony, coupled with testimony from other witnesses and evidence recovered from the defendant's room, formed a legally sufficient basis to convict the defendant on the criminal gang enhancement charge.

People v. Chavez, 2010 Cal. App. Unpub. LEXIS 6186 (Cal. Ct. App. 2010),[21] upheld information charging the defendant's involvement with a criminal street gang. An investigator from the district attorney's office was qualified as a gang expert at trial and testified to common characteristics of gang members and how to identify them. As part of the expert's conclusion that the defendant was an active gang member, the expert relied on a MySpace posting containing a picture of the defendant, the name of the gang, and the defendant's gang moniker. The MySpace evidence and testimony of the expert provided enough of a basis for the information to survive dismissal challenges. See also ***People v. Corleone***, 2009 Cal. App. Unpub. LEXIS 3107 (Cal. Ct. App. 2009)[22] (stalking and criminal threat convictions upheld based on MySpace, e-mail, and text-message evidence); ***People v. Abusharif***, 2011 Ill. App. Unpub. LEXIS 853 (Ill. App. Ct. 2011)[23] (trial court did not abuse discretion in admitting text message and MySpace message evidence in murder trial).

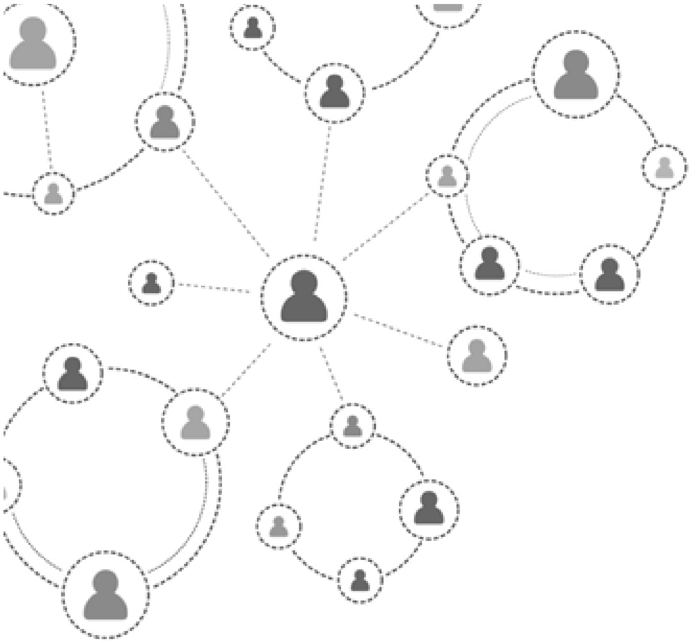
U.S. v. McNamara-Harvey, 2010 U.S. Dist. LEXIS 106141 (E. D. Pa. 2010). Anonymous tips that the defendant posted pro-Palestinian/anti-Israeli videos on his Facebook page, as well as personal admissions from the defendant to the Federal Bureau of Investigation (FBI) that he had posted disturbing and/or extremist videos, helped form the basis of a warrant for computer-based evidence of potential terroristic acts.

[21] This is an unpublished opinion. Please check local court rules when relying on this opinion as authority.

[22] See Footnote 21.

[23] See Footnote 21.

Griffin v. Maryland, 2011 Md. LEXIS 226 (Md. 2011). The appeals court ruled that MySpace pages were erroneously admitted into evidence because they had not been properly authenticated. The trial court admitted the postings based on a police officer's testimony that the picture in the profile was of the purported owner and they had the same location and date of birth. The picture, location, and birth date did not constitute sufficient "distinctive characteristics" to properly authenticate the MySpace printouts of the profile and posting because of the possibility that someone else could have made the profile or had access to it to make the posting. The court stated that there are different concerns when authenticating printouts from social media sites that go beyond the authentication concerns of e-mails, Internet chats, and text messages. Some suggested approaches to the social media authentication issue include an admission of the purported profile owner that it is his or her profile and he/she made the postings in question, a search of the person's computer and Internet history that links the subject to the profile or post, or information obtained directly from the social media site that identifies the person as the profile's owner and individual with control over it, possibly including IP address identification information.



Appendix B—Georgia Bureau of Investigation Social Media Policy

Georgia Bureau Of Investigation Investigative Division
Directive 8-6-5

Title: Guidelines For The Use Of Social Media By The Investigative Division

Date: October 26, 2012

Reviewed: October 26, 2012

Authority: R. E. Andrews
Deputy Director For Investigations

Page 1 of 12

Purpose: To establish guidelines for the use of social media in pre-employment background investigations, crime analysis and situational assessments, criminal intelligence development, and criminal investigations.

Definitions

Crime Analysis and Situational Assessment Reports—Analytic activities to enable GBI to identify and understand trends, causes, and potential indicia of criminal activity, including terrorism.

Criminal Intelligence Information—Data which meets criminal intelligence collection criteria and which has been evaluated and determined to be relevant to the identification of criminal activity engaged in by individuals who or organizations which are reasonably suspected of involvement in criminal activity.

Criminal Nexus—Established when behavior or circumstances are related to an individual or organization's involvement or planned involvement in criminal activity or enterprise.

Online Alias—An online identity encompassing identifiers, such as name and date of birth, differing from the employee's actual identifiers, that uses a nongovernmental Internet Protocol address. Online alias may be used to monitor activity on social media websites or to engage in authorized online undercover activity.

Online Undercover Activity—The utilization of an online alias to engage in interactions with a person via social media sites that may or may not be in the public domain (i.e. "friending a person on Facebook").

Public Domain—Any Internet resource that is open and available to anyone.

Social Media—A category of Internet-based resources that integrate user-generated content and user participation. This includes, but is not limited to, social media networking sites (Facebook, MySpace), micro blogging sites (Twitter), photo- and video-sharing sites (Flickr, YouTube), wikis (Wikipedia), blogs, and news sites (Digg, Reddit).

Social Media Monitoring Tool—A tool used to capture data and monitor social media sites by utilizing automated tools such as web crawlers and word search functions to make predictive analysis, develop trends, or collect information. Examples include Netbase, Twitterfall, Trackur, Tweetdeck, Socialmention, Socialpointer, and Plancast.

Social Media Websites—Sites which focus on building online communities of people who share interests and activities and/or exploring the interests and activities of others. Social media websites are further categorized by Internet-based resources that integrate user-generated content and user participation. This includes, but is not limited to, social networking sites (Facebook, MySpace), micro blogging sites (Twitter, Nixle), photo-and video-sharing sites (Flickr, YouTube), wikis (Wikipedia), blogs, and news sites (Digg, Reddit). The absence of an explicit reference to a specific social media website does not limit the application of this policy.

Valid Law Enforcement Purpose—A purpose for information/intelligence gathering development, or collection, use, retention, or sharing that furthers the authorized functions and activities of a law enforcement agency, which may include the prevention of crime, ensuring the safety of the public, furthering officer safety, and homeland and national security, while adhering to law and agency policy designed to protect the privacy, civil rights, and civil liberties of Americans.

I. GENERAL

Social media may be a valuable investigative tool to detect and prevent criminal activity. Social media has been used for community outreach events such as providing crime prevention tips, providing crime maps, and soliciting tips about unsolved crimes. Social media may also be used to make time sensitive notifications regarding special events, weather emergencies, or missing or endangered persons. While social media is a new resource for law enforcement, employees must adhere to this policy to protect individuals' privacy, civil rights, and civil liberties and to prevent employee misconduct.

II. UTILIZATION OF SOCIAL MEDIA

A. **Social media may be used by Investigative Division personnel for a valid law enforcement purpose. The following are valid law enforcement purposes:**

1. Pre-employment background investigations;
2. Crime analysis and situational assessment reports;
3. Criminal intelligence development; and
4. Criminal investigations.

B. **While on duty, employees will utilize social media, access social media websites, online aliases, and social media monitoring tools only for a valid law enforcement purpose. The utilization of an online alias or social media monitoring tool for personal use is prohibited and is considered employee misconduct.**

C. **Employees will only utilize social media to seek or retain information that:**

1. Is based upon a criminal predicate or threat to public safety; or
2. Is based upon reasonable suspicion that an identifiable individual, regardless of citizenship or U.S. residency status, or organization has committed an identifiable criminal offense or is involved in or is planning criminal conduct or activity that presents a threat to any individual, the community, or the nation and the information is relevant to the criminal conduct or activity (criminal intelligence information); or
3. Is relevant to the investigation and prosecution of suspected criminal incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime; or
4. Is useful in crime analysis or situational assessment reports for the administration of criminal justice and public safety; or
5. Is relevant to pre-employment background investigations.

D. **The GBI will not utilize social media to seek or retain information about:**

1. Individuals or organizations solely on the basis of their religious, political, social views or activities; or
2. An individual's participation in a particular non-criminal organization or lawful event; or
3. An individual's race, ethnicity, citizenship, place of origin, disability, gender, or sexual orientation unless such information is relevant to the individual's criminal conduct or activity or if required to identify the individual; or
4. An individual's age other than to determine if someone is a minor.

E. **The GBI will not directly or indirectly receive, seek, accept, or retain information from:**

1. An individual or nongovernmental information provider who may or may not receive a fee or benefit for providing the information if there is reason to believe that the information provider is legally prohibited from obtaining or disclosing the information; or
2. A source that used prohibited means to gather the information.

III. AUTHORIZATION TO ACCESS SOCIAL MEDIA WEBSITES

This section addresses the authorization necessary to utilize social media and access social media websites for crime analysis and situational awareness/assessment reports; intelligence development; and criminal investigations.

A. Public Domain

No authorization is necessary for general research, topical information or other law enforcement uses that do not require the acquisition of an online alias.

B. Online Alias

An online alias may only be used to seek or retain information that:

1. Is based upon a criminal predicate or threat to public safety; or

2. Is based upon reasonable suspicion that an identifiable individual, regardless of citizenship or U.S. residency status, or organization has committed a criminal offense or is involved in or is planning criminal conduct or activity that presents a threat to any individual, the community, or the nation and the information is relevant to the criminal conduct or activity; or

3. Is relevant to the investigation and prosecution of suspected criminal incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime; or

4. Is useful in crime analysis or situational assessment reports for the administration of criminal justice and public safety.

C. Authorization for Online Aliases

Sworn agents or criminal intelligence analysts must submit a request for an online alias. No other Investigative Division personnel are authorized to submit requests for an online alias or to use an online alias in the performance of their official duties.

The request must contain the following information:

1. Purpose for the request (i.e. type of investigative activity);

2. Username;

3. Identifiers and pedigree to be utilized for the online alias, such as email address, username and date of birth. Do not include password(s) for online aliases and ensure password(s) are secured at all times; and

4. Photograph to be used with online alias, if applicable.

The work unit supervisor must evaluate the request to determine whether an online alias would serve a valid law enforcement purpose. The work unit supervisor must maintain the requests for online alias and their status (approved/denied) for two years from the date of deactivation of the online alias.

Investigative Division personnel with an approved online alias may use their online alias to make false representations in concealment of personal identity in order to establish social media accounts (i.e. a Facebook account). The establishment of a social media account with an approved online alias must be documented.

D. Authorization for Online Undercover Activity

1. A sworn agent who has an authorized online alias may also request authorization to engage in online undercover activity. Only agents will be authorized to engage in online undercover activity utilizing the online alias.

2. Online undercover activity occurs when the agent utilizing the online alias interacts with a person via social media. Online undercover operations will only be utilized when there is reason to believe that criminal offenses have been, will be or are being committed (e.g. internet chat rooms where child exploitation occurs).

3. Employees must submit a request to engage in online undercover activity. The request must contain the following information:

   a. Online alias(es) to be used in the online undercover activity;

   b. Social media accounts utilized;

   c. Valid law enforcement purpose; and

   d. Anticipated duration for the online undercover activity.

4. The work unit supervisor must evaluate the request to determine whether online undercover activity is appropriate. If the request is approved, the authorization must be maintained in the file containing the record of the online undercover activity.

5. In situations involving exigent circumstances, the work unit supervisor may provide verbal authorization for online undercover activity. The work unit supervisor should provide written documentation of the request, the exigent circumstances, and the circumstances of the verbal authorization as soon as practical.

6. A record will be maintained of all online undercover activity.

7. Once authorized to engage in online undercover activity, the agent should utilize the appropriate deconfliction system.

8. All approved online undercover activity requests will be reviewed monthly by the work unit supervisor to ensure continued need for the online undercover activity. Approved online undercover activity that does not provide information regarding a valid law enforcement purpose within thirty (30) days will be discontinued.

9. A summary will be placed in the file indicating the date of termination of the online undercover activity. The online alias may be maintained if it is anticipated that it will be utilized again.

IV. AUTHORIZATION TO UTILIZE SOCIAL MEDIA MONITORING TOOLS

A. Prior to utilizing a social media monitoring tool, the work unit supervisor will submit a request through the chain of command to the Deputy Director for Investigations for authorization to use the social media monitoring tool. The social media monitoring tool may be utilized in criminal investigations; criminal intelligence development; and crime analysis and situational assessment reports (e.g. during sporting events, demonstrations or other large gatherings that require a law enforcement presence to ensure the safety of the public). The request must contain the following:

1. A description of the social media monitoring tool;

2. Its purpose and intended use;

3. The social media websites the tool will access;

4. Whether the tool is accessing information in the public domain or information protected by privacy settings; and

5. Whether information will be retained by the GBI and if so, the applicable retention period for such information.

B. The request must be reviewed by the GBI Privacy Officer prior to approval.

C. In exigent circumstances, the work unit supervisor may obtain verbal authorization to utilize the social media monitoring tool and provide written documentation as soon as practical. The written documentation should include a description of the exigent circumstances and the verbal authorization, as well as the required information for the request.

D. If approved, the social media monitoring tool may be utilized for a period of ninety (90) days or, in the case of situational assessments such as an event or large gathering, until the conclusion of the law enforcement activity related to the event. After ninety (90) days, the work unit supervisor must submit a summary describing the law enforcement actions that resulted from the use of the social media monitoring tool.

If continued use is needed, the summary may also contain a request to continue using the social media monitoring tool. The process to approve the request is the same as the original request.

V. SOURCE RELIABILITY AND CONTENT VALIDITY

Information developed from social media sites should be corroborated using traditional investigative tools including interviews, verification of address, verification of internet protocol address information, or other lawful means.

VI. DOCUMENTATION AND RETENTION

Other than crime analysis and situational assessment reports, all information obtained from social media websites shall be placed within a case file, suspicious activity report, or intelligence report. At no time should Investigative Division personnel maintain any social media files outside of these authorized files.

Crime analysis and situational assessment reports may be prepared for special events management, including First Amendment-protected activities. At the conclusion of the situation requiring the report or First Amendment-protected event where there was no criminal activity related to the information gathered, the information obtained from the social media monitoring tool will be retained for no more than fourteen (14) days. Information from the social media monitoring tool that does indicate a criminal nexus will be retained in an intelligence report, suspicious activity report, or case investigative file as directed by the State of Georgia retention schedule.

Information identified as criminal in nature that is obtained in the course of an investigation from a social media site will be collected and retained using screen shots, printouts of chat logs, copying uniform resource locators (URL's) for subpoena or investigatory purposes, or storing the information via secure digital means. When possible, employees will utilize investigative computer systems and software intended to record data from social media sites.

VII. OFF DUTY CONDUCT

A. An employee who becomes aware of potential criminal activity via the Internet while off duty shall contact their supervisor or CEACC if the activity involves a minor child or exigent circumstances to determine the best course of action.

B. As soon as practical following awareness of the potential criminal activity, the employee should prepare detailed notes to document a complete description of the information observed and specifics as to the events that occurred or action taken.

C. Employees shall act to preserve and maintain proper custody of images, texts, photographs, or other potential evidence.

VIII. PERSONAL EQUIPMENT AND PERSONAL SOCIAL MEDIA WEBSITES AND PASSWORDS

Given the ease with which information can be gathered from public internet searches, tracking services, and other computer analytic technology, the use of employee's personal or family internet accounts, social media, or internet service for official GBI business is prohibited.

IX. DISSEMINATION

Retention and dissemination of social media information will be the same as the type of file, whether a paper or electronic file, in which the information is located. For example, retention and dissemination of social media information within an intelligence file will be treated in the same manner as an intelligence file. Information developed during the course of a criminal investigation will be located in the investigative case file and retained and disseminated in the same manner as the investigative case file.

X. EMPLOYMENT BACKGROUND INVESTIGATIONS

As part of its employment background process, Investigative Division personnel will conduct a search of social media websites and profiles in the public domain regarding the applicant. Applicants will be notified that this search will be conducted. Applicants are not required to disclose passwords to social media sites or profiles to the GBI. In the event an applicant discloses their password, the GBI will not utilize the password to log into the applicant's social media site or profile. Employees will not search or attempt to gain access to private social media profiles.

All searches of applicant social media pages and profiles will only search information that is in the public domain.

Online aliases will not be used to conduct employment background investigations.

Only criminal comments or images will be collected as part of the background investigatory process. Employees will not collect or maintain information about the political, religious, or social views, associations or activities of any individual or any group unless such information directly relates to criminal conduct or activity.

During the course of a background investigation, if a reference, supervisor, or colleague of the applicant provides negative information on the applicant related to a social media site, the agent will prepare an investigative summary outlining the information provided by the reference.

XI. SANCTIONS FOR MISUSE

Any employee who violates the provisions of this directive will be subject to disciplinary action, up to and including termination.

XII. COMPLAINTS AND INFORMATION QUALITY ASSURANCE

Employees will report violations or suspected violations of this directive to the Privacy Officer in accordance with the GBI Privacy Policy, Directive 7-6 Criminal Intelligence and Privacy Protections, Section VI (D).

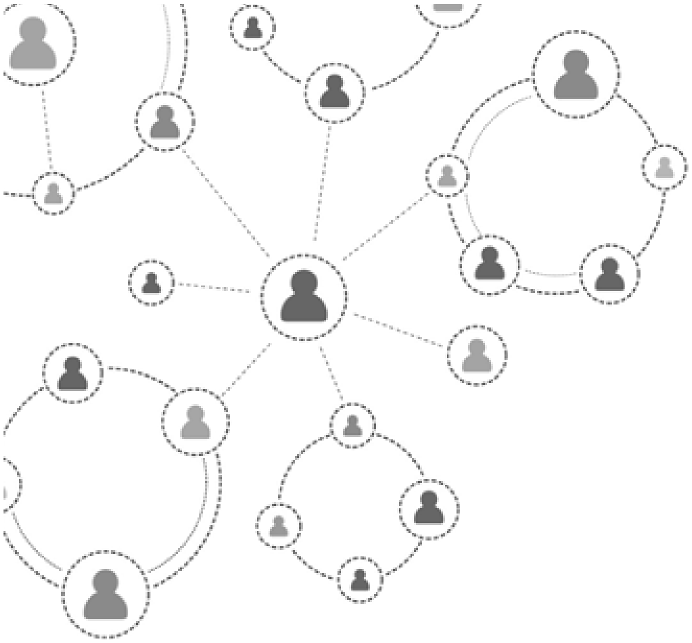
Complaints from the public regarding information obtained from social media websites will be submitted to the Privacy Officer and handled in accordance with the GBI Privacy Policy. If the information is determined to be erroneous, the information will be corrected or deleted.

XIII. AUDIT

As part of the GBI annual privacy audit, compliance with this directive will be verified by a GBI inspection team led by the Privacy Officer.

XIV. ANNUAL REVIEW

The GBI Privacy Officer will review this directive at least annually and direct the updating of the policy and procedures as necessary.



Appendix C—Dunwoody Police Department Social Media Policy

Dunwoody Police Department Standard Operating Procedure

Subject	Social Media
Effective Date	November 15, 2011
Sop #	A-50
Reference	Social Media Pages, Blogs, Twitter, Departmental Material, Agency And Personnel Electronic Devices
Special Instructions	Annual Review
Distribution	All Personnel
# Pages	4

I. PURPOSE

The department endorses the use of social media to enhance communication, collaboration, and information exchange; streamline processes; and foster productivity. This policy establishes the department's position on the utility of social media, including management, administration, and oversight. This policy is intended to address social media in general, not a particular form of social media.

II. POLICY

Social media provides a potentially valuable means of assisting the department and department personnel in meeting community outreach, problem-solving, investigative, crime prevention, and related goals of the department. This policy identifies potential uses that may be explored or expanded upon as directed by the Chief of Police. The personal use of social media can have a bearing on department personnel in their official capacity. As such, this policy provides information of a precautionary nature as well as prohibitions on the use of social media by department personnel.

III. DEFINITIONS

Blog—A self-published commentary on a particular topic that may allow visitors to post responses, reactions, or comments. This term is short for "Web log."

Page—The specific portion of a social media website where content is displayed and managed by an individual or individuals.

Post—Content an individual shares on a social media site or the act of publishing content on a site.

Profile—Information that a user shares about himself or herself on a social networking site.

Social Media—A category of Internet-based resources that integrate user-generated content and user participation. This includes, but is not limited to, social networking sites (Facebook, MySpace), microblogging sites (Twitter, Nixle), photo- and video-sharing sites (Flicker, YouTube), wikis (Wikipedia), blogs, and news sites (Digg, Reddit).

Social Networks—Online platforms where users can create profiles, share information, and socialize with others user a range of techniques.

Speech—Expression or communication of thoughts or opinions in spoken words, in writing, by expressive conduct, symbolism, photographs, videotape, or related forms of communication.

Electronic Communications—Electronic Communications include, among other things, messages, images, data or any other information used in e-mail, instant messages, voice mail, fax machines, computers, personnel digital assistants (including Blackberry or similar text messaging devices), pagers, telephones, cellular and mobile phones including those with cameras, intranet, Internet, back-up storage, information on a memory or flash key or card, jump or zip drive, any other type of internal or external removable storage drives or any other technology tool. In the remainder of this policy, all of these communication devices are collectively referred to as "Systems."

IV. PROCEDURES

A. On-the-Job Use / Social Media

Department-Sanctioned Presence:

1. All department social media sites or pages shall be approved by the Chief of Police in accordance with City of Dunwoody policies.
2. Social media pages shall clearly indicate they are maintained by the department and shall have department contact information displayed.
3. Social media content shall adhere to applicable laws, regulations, and policies, including information technology and records management policies.
4. Content of social media pages is subject to Open Records laws.
5. Department personnel representing the department via social media outlets shall conduct themselves as representatives of the department and the City of Dunwoody and shall adhere to all department and City standards of conduct. They shall identify themselves as members of the department; not make comments regarding the guilt or innocence of suspects or arrestees; not make comments concerning pending prosecutions and not post, transmit or otherwise disseminate confidential information, including pictures, videos, evidence, or other materials in the department relating to training, work assignments, and enforcement efforts without the express written permission of the Chief of Police.
6. Department personnel shall not conduct political activities or private business on departmental social media.
7. The use of departmental computers, telephones, and other electronic communications devices to access social media is prohibited without the authorization of the Chief of Police.

8. Department personnel shall use personal electronic communications devices and computers to manage the department's social media sites only with the express written permission of the Chief of Police.

9. Department personnel shall observe and abide by all copyright, trademark, and service mark restrictions in posting materials to electronic media.

Social media is a valuable tool when seeking evidence or information regarding missing persons, wanted persons, gang activity, crimes perpetrated online, photographs or videos of a crime posted by a participant or observer.

10. Social media can be used for community outreach by providing crime prevention tips, offering online reporting opportunities, sharing crime maps and data, and soliciting tips about unsolved crimes.

11. Social media may be used for time-sensitive notifications of road closures, special events, weather emergencies, and missing or endangered persons.

B. Personal Use / Social Media

Precautions and Prohibitions:

1. Department personnel are free to express themselves as private citizens on social media sites to the degree that their speech does not impair the work of the department for which confidentiality is important and does not impede the performance of duties.

2. Department personnel are cautioned that representing themselves as employees of the department in their off duty social networking may bring about targeting of the employee. The targeting of law enforcement personnel through social networking sites as a form of retaliation is documented.

3. Department personnel are cautioned that when using social media, their speech becomes part of worldwide electronic domain. Posting of personal photographs and other personal information by departmental personnel may subject them to becoming targets of criminal acts, harassment, or other forms of abuse due to their employment.

4. Department personnel shall adhere to the Code of Conduct when representing themselves as members of the department. They shall not post obscene or sexually explicit language, images, or acts and statements or other forms of speech that ridicule, malign, disparage, or otherwise express bias against any race, any religion, or any protected class of individuals.

5. Department personnel may not divulge information gained by reason of their authority; make statements, speeches, appearances, and endorsements; or publish materials that could reasonably be considered to represent the views or positions of this department without express authorization of the Chief of Police.

C. Agency and Personnel Electronic Devices

Personal Computers, Cell Phones, and Recording Devices:

1. Department personnel and system users may not use personal laptops within any City building or leased space. Additionally, employees and system users may not use personal laptops to gain access to City network resources. Department personnel may have extenuating reasons for using a personal laptop, which must be approved by the Chief of Police.

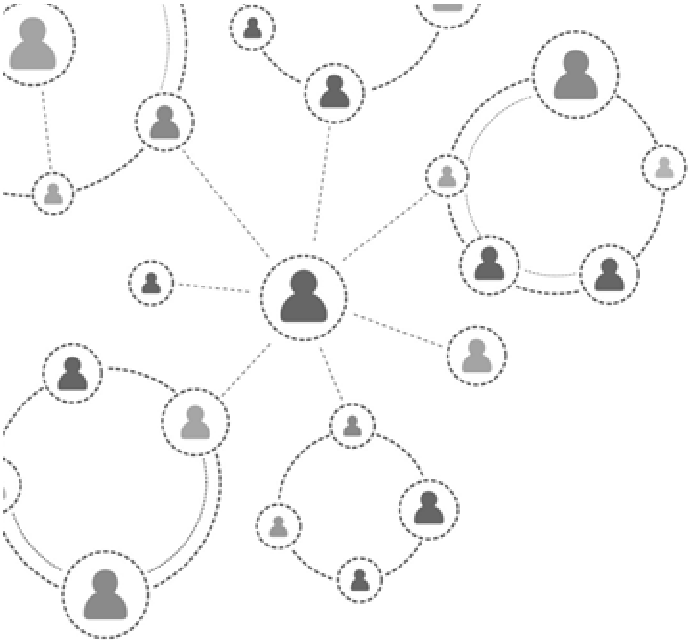
2. Although incidental and occasional personal use of Systems that does not interfere or conflict with productivity or the City's business or violate City policy is permitted, personal communications in our Systems are treated the same as all other Electronic Communications and will be used, accessed, recorded, monitored, and disclosed by the City at any time without further notice. Since all Electronic Communications and Systems can be accessed without advance notice, employees and system users

should not use our Systems for communication or information that they would not want revealed to third parties. Employees, therefor, shall not have any expectation of privacy regarding the use of our Systems.

3. The use of personal audio / visual recording devices while on duty and for the performance of assigned duties and responsibilities is prohibited unless otherwise authorized in writing by the Chief of Police.

Billy Grogan, Chief of Police
Dunwoody Police Department

First Reading:	091111
Final Adoption	101311
Distribution Date	101411
Effective Date	111511



Appendix D— New York City Police Department Social Media Policy

Data contained within social network sites may assist law enforcement in gathering timely information in furtherance of crime prevention, preservation of public order, and the investigation of criminal activity, including suspected terrorist activity. These guidelines are promulgated, in part, to instill the proper balance between the investigative potential of social network sites and privacy expectations.

Therefore, effective immediately, when a member of the service requires the use of social network websites to conduct investigations or research, the following procedure will be complied with:

I. Purpose

To conduct social network-based investigations and research.

II. Scope

Data contained on the Internet within social network sites may assist law enforcement in gathering timely information in furtherance of crime prevention, including the preservation of public order and the investigation of criminal activity, including suspected terrorist activity. To effectively fulfill these duties, it may be necessary for members of the service to access social network sites using an online alias. No prior authorization is ever required for information contained on publicly available internet sources.

III. Definitions

Exigent Circumstances—For the purpose of this procedure, circumstances requiring action before authorization can be obtained, in order to protect life or substantial property interest; to apprehend or identify a fleeing offender; to prevent the hiding, destruction or alteration of evidence; or to avoid other serious impairment or hindrance of an investigation.

Online Alias—An online identity encompassing identifiers, such as name and date of birth, differing from the user's actual name, date of birth, or other identifiers.

Online Alias Access—Internet-based searches involving the search and acquisition of information from sites that require an email address, password, or other identifiers for which an online alias is utilized.

Public Domain Data—Information accessible through the Internet for which no password, email address, or other identifier is necessary to acquire access to view or collect such information.

Social Network Site—Online platform where users can create profiles, share information, or socialize with others using a range of technologies.

Procedure

When a member of the service requires access to a social network website for investigative or research purposes:

Member of the Service

1. **Confer with supervisor, if access to public domain data requires the use of an online alias/online alias access.**
    a. No conferral or authorization is required for general research, topical information or other general uses that do not require the acquisition of an online alias/online alias access.

If application for online alias does not involve suspected terrorist activity:

Supervisor

2. **Evaluate request to determine whether an online alias would serve an investigative purpose, and if so, prepare Typed Letterhead requesting an online alias to bureau chief/deputy commissioner concerned.**

2. **Include on Typed Letterhead:**
    a. Purpose for the request (i.e., type of investigation, etc.)
    b. Tax registry number of requesting member
    c. Username (online alias)
    d. Identifiers and pedigree to be utilized for the online alias, such as email address, username and date of birth.
    e. Do not include password(s) for online alias and ensure password(s) are secured at all times.
    f. Indicate whether there is a need to requisition a Department laptop with aircard.

4. **Review photograph to be used in conjunction with online alias, if applicable.**
    a. Consider the purpose for which the photograph is being used and the source of the photograph.
    b. Attach a copy of the approved photograph and indicate on Typed Letterhead how photograph was obtained.

5. **Forward request to commanding officer for review.**

Commanding Officer

6. **Review request(s) and consider the purpose and whether granting approval would serve an investigative purpose.**

7. **Endorse request(s) indicating APPROVAL/DISAPPROVAL within one day of original request and if APPROVED, immediately forward approval to bureau chief/deputy commissioner concerned, through channels, for informational purposes.**

8. **File copies of requests in command.**

Member of the Service

9. Maintain record of online alias in case records management systems or appropriate Department records.

Bureau Chief/Deputy Commissioner

10. Maintain folder for each APPROVED online alias.

a. Designate an administrator for the online alias.

If application for online alias involves suspected terrorist activity:

Supervisor

11. Immediately contact Intelligence Division, Operations Desk supervisor and provide details regarding proposed investigation.

Intelligence Division, Operations Desk Supervisor

12. Determine if investigation should be conducted by the Intelligence Division and proceed accordingly.

13. Notify requesting supervisor to proceed with investigation if it has been determined that the investigation will not be conducted by the Intelligence Division.

Supervisor

14. Comply with steps "2" through "10", as appropriate, if investigation will not be conducted by the Intelligence Division.

When exigent circumstances exist that would warrant the immediate use of an online alias:

Supervisor

15. Confer with Intelligence Division, Operations Desk supervisor, if there is concern that the investigation may involve suspected terrorist activity.

a. Comply with instructions from Intelligence Division, Operations Desk supervisor.

16. Confer with commanding officer/executive officer, if investigation does not involve suspected terrorist activity.

17. Instruct member of the service to proceed with investigation upon receiving APPROVAL from commanding officer/executive officer.

a. Comply with steps "2" through "10", as appropriate, and include in Typed Letterhead, the circumstances that led to the determination of exigent circumstances.

Additional Data

Legal Considerations

During the course of an investigation, a member of service may need access to information regarding online accounts maintained by service providers. The federal Electronic Communications Privacy Act (ECPA) governs seizures of electronic evidence. Some information may be obtained with a subpoena; other information requires a special court order; and still other information requires a search warrant. Pertinent sections of the ECPA are as follows:

a. A subpoena is generally deemed sufficient to obtain information such as user information and payment records.

b. Electronic communications, such as email content, in electronic storage for 180 days or less may be obtained only after the issuance of a search warrant, and delayed notification to the subscriber or customer may be ordered if specifically requested in the search warrant application.

c. Electronic communications in electronic storage for more than 180 days may be obtained with a subpoena signed by a judge; however, notice must be provided to the subscriber or customer unless the electronic communications are obtained after the issuance of a search warrant allowing for delayed notification.

Additional Data (continued)

d. In anticipation of the issuance of a search warrant, a member of the service may send a request known as a "preservation letter" to an electronic service provider requesting the preservation of electronic records for 90 days, and extend the request for an additional 90 day period.

Note that particular service providers are known to ignore non-disclosure orders (i.e., some service providers will disclose the existence of a search warrant or subpoenas to a subject subscriber or customer.) In general, members of the service should consult with the Legal Bureau before seeking electronic communication through a search warrant or otherwise.

Data obtained through a grand jury subpoena or court order cannot be shared with other law enforcement agencies unless otherwise authorized.

Operational Considerations

When a member of the service accesses any social media site using a Department network connection, there is a risk that the Department can be identified as the user of the social media. Given this possibility of identification during an investigation, members of the service should be aware that Department issued laptops with aircards have been configured to avoid detection and are available from the Management Information Systems Division (MISD). A confidential Internet connection (e.g., Department laptop with aircard) will aid in maintaining confidentiality during an investigation. Members who require a laptop with aircard to complete the investigation shall contact MISD Help Desk, upon APPROVAL of investigation, and provide required information.

In addition to using a Department laptop with aircard, members of the service are urged to take the following precautionary measures:

a. Avoid the use of a username or password that can be traced back to the member of the service or the Department;

b. Exercise caution when clicking on links in tweets, posts, and online advertisements;

c. Delete "spam" email without opening the email; and

d. Never open attachments to email unless the sender is known to the member of the service.

Furthermore, recognizing the ease with which information can be gathered from minimal effort from an Internet search, the Department advises members against the use of personal, family, or other non-Department Internet accounts or ISP access for Department business. Such access creates the possibility that the member's identity may be exposed to others through simple search and counter-surveillance techniques.

Department Policy

The “Handschu Consent Decree” and “Guidelines for Investigations Involving Political Activity” (see Appendix “A” and “B” of Interim Order 58, series 2004, “Revision to Patrol Guide 212-72, ‘Guidelines for Uniformed Members of the Service Conducting Investigations of Unlawful Political Activities’”) require that any investigation, including investigations on social networks, by the New York City Police Department involving political activity shall be initiated by and conducted only under the supervision of the Intelligence Division. Accordingly, members of the service shall not conduct investigations on social networks involving political activity without the express written approval of the Deputy Commissioner, Intelligence. Any member of the service who is uncertain whether a particular investigation constitutes an “investigation involving political activity” shall consult with the Legal Bureau.

Members of the service who have created and used online aliases prior to the promulgation of this procedure must submit a request to continue utilizing the alias in accordance with this procedure.

Related Procedures

- Citywide Intelligence Reporting System (P.G. 212-12)
- Guidelines for Uniformed Members of the Service Conducting Investigations of Unlawful Political Activities (Interim Order 58, series 2004)

Forms and Reports

Typed Letterhead

Commanding officers will ensure that the contents of this Order are brought to the attention of members of their commands.

By Direction Of The Police Commissioner

Distribution

All Commands

About the Global Advisory Committee

The Global Advisory Committee (GAC) serves as a Federal Advisory Committee to the U.S. Attorney General. Through recommendations to the Bureau of Justice Assistance (BJA), the GAC supports standards-based electronic information exchanges that provide justice and public safety communities with timely, accurate, complete, and accessible information, appropriately shared in a secure and trusted environment. GAC recommendations support the mission of the U.S. Department of Justice, initiatives sponsored by BJA, and related activities sponsored by BJA's Global Justice Information Sharing Initiative (Global). BJA engages GAC-member organizations and the constituents they serve through collaborative efforts, such as Global working groups, to help address critical justice information sharing issues for the benefit of practitioners in the field.

Issued 02/13

APPENDIX IV

IACP
CENTER FOR
SOCIAL MEDIA

SUPPORTING THE NEEDS OF LAW ENFORCEMENT ONLINE

2012 IACP Social Media Survey

In August 2012, the IACP conducted its annual survey on law enforcement's use of social media. The survey addressed the current state of practice and the issues law enforcement agencies are facing in terms of social media. The survey was sent electronically to law enforcement executives across the United States. There are 600 law enforcement agencies from 48 states represented in the survey results.

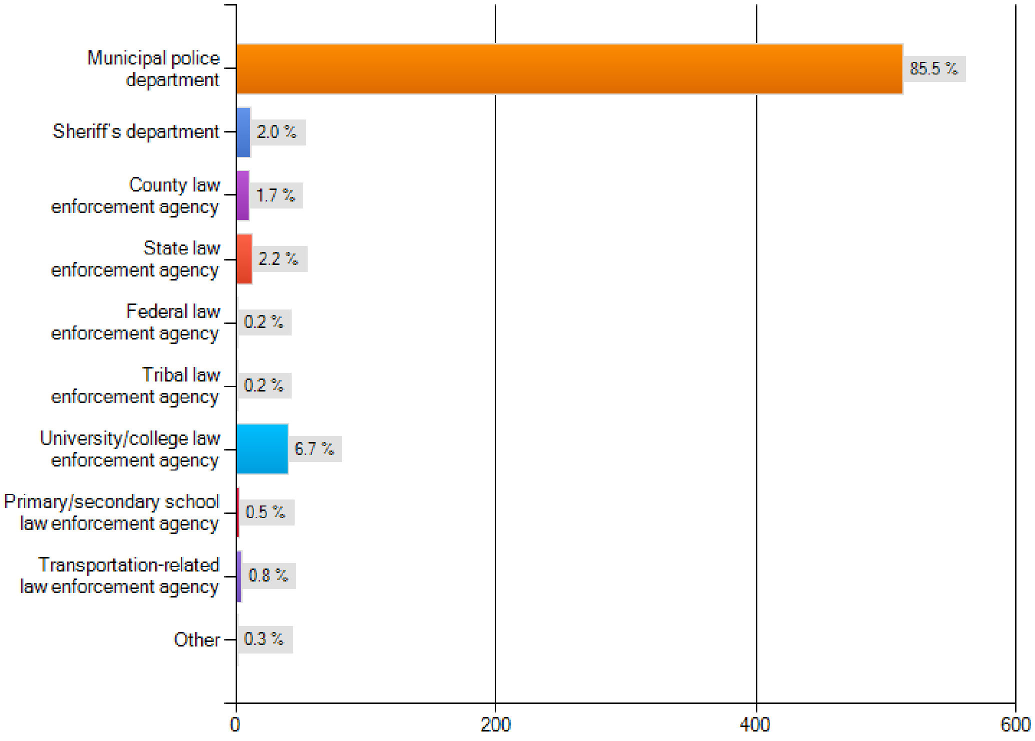
For more information about this survey or the IACP Center for Social Media visit www.IACPsocialmedia.org or e-mail socialmedia@theiacp.org.

SURVEY HIGHLIGHTS

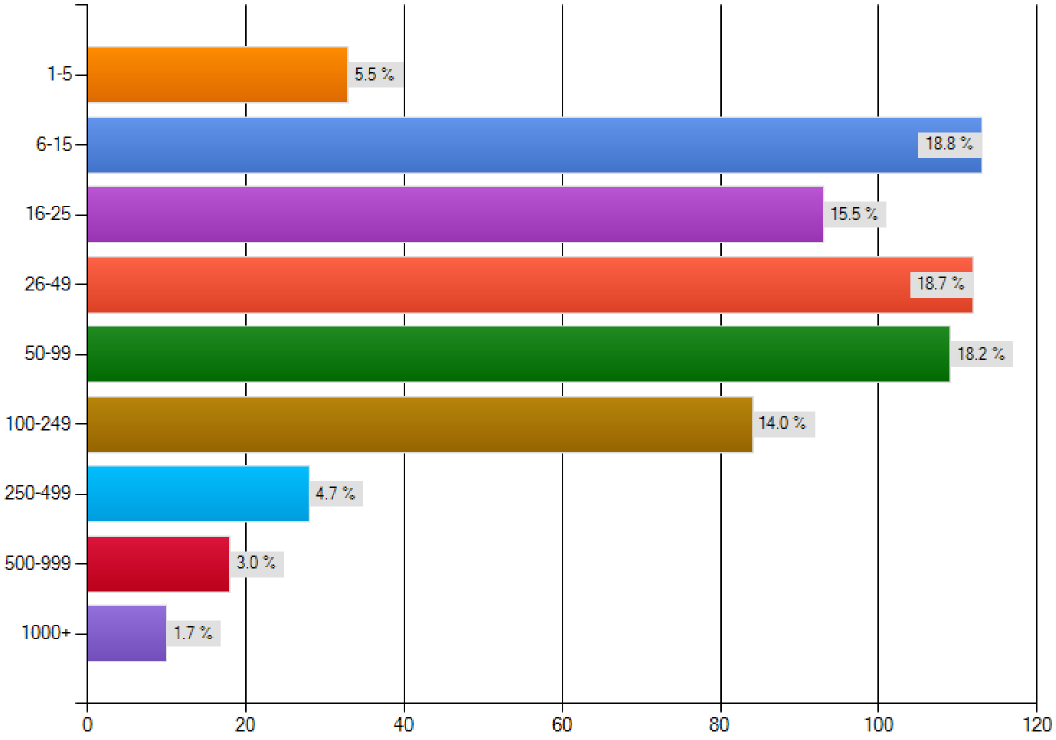
- 92.4 percent of agencies surveyed use social media.
- The most common social media use by survey respondents was for criminal investigations, 77.1 percent.
- 56.3 percent of the agencies not currently using social media are considering its adoption.
- 61.9 percent of agencies surveyed have a social media policy and an additional 18.9 percent are in the process of developing a policy.
- 60 percent of agencies are either somewhat concerned or very concerned about online radicalization and violent extremism.
- 74 percent of agencies report that social media has helped solve crimes in their jurisdiction.

Demographic Information

Which of the following best describes your agency?

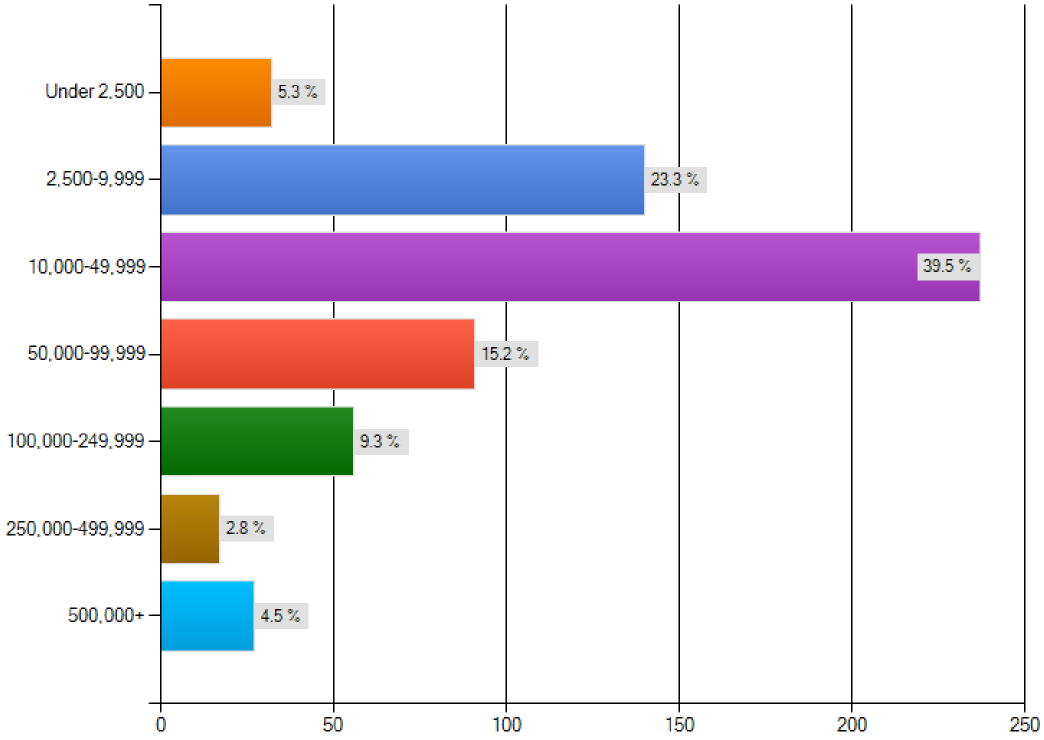


Please indicate the number of full-time sworn personnel in your agency.

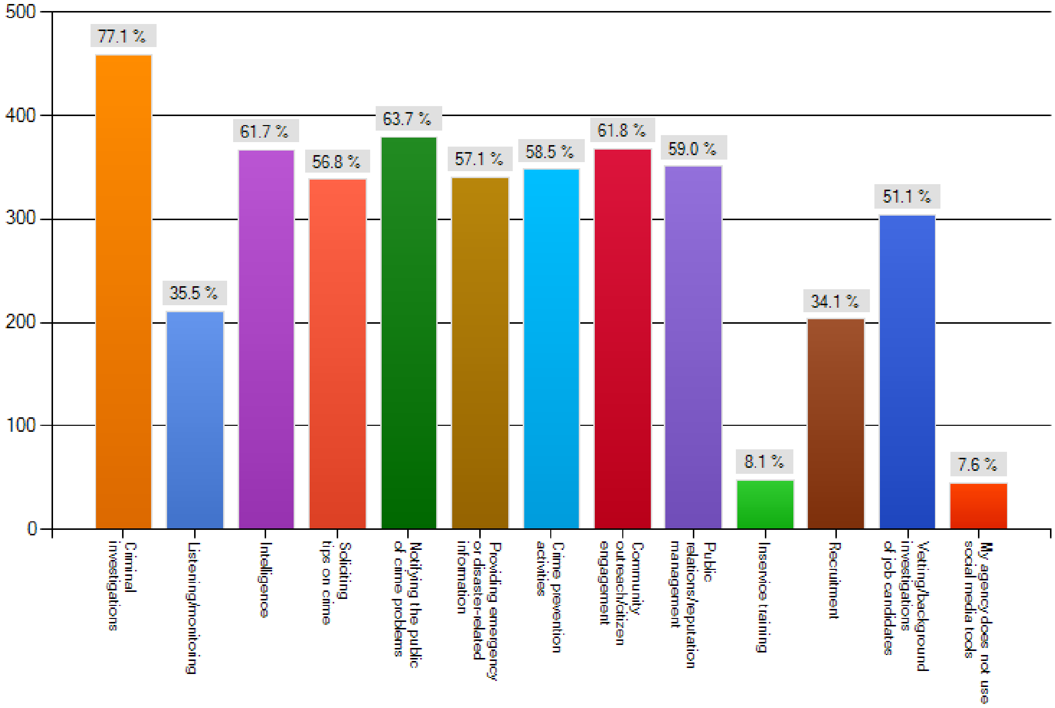


DEMOGRAPHIC INFORMATION

Please indicate the population served by your agency.

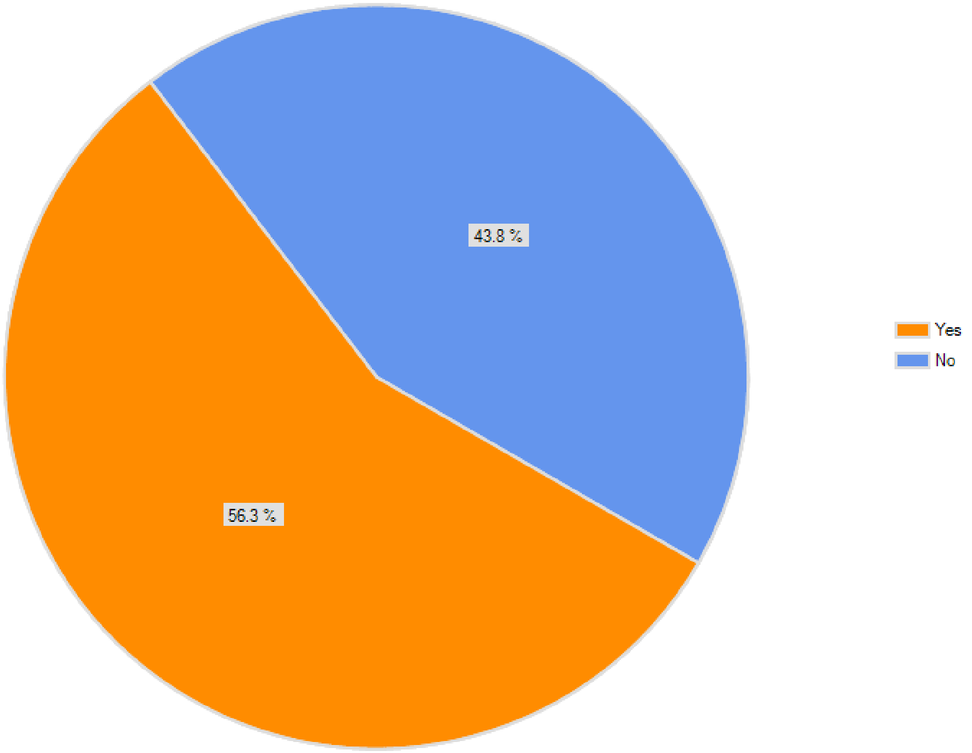


Which of the following activities does your agency use social media tools for? (Select all that apply)

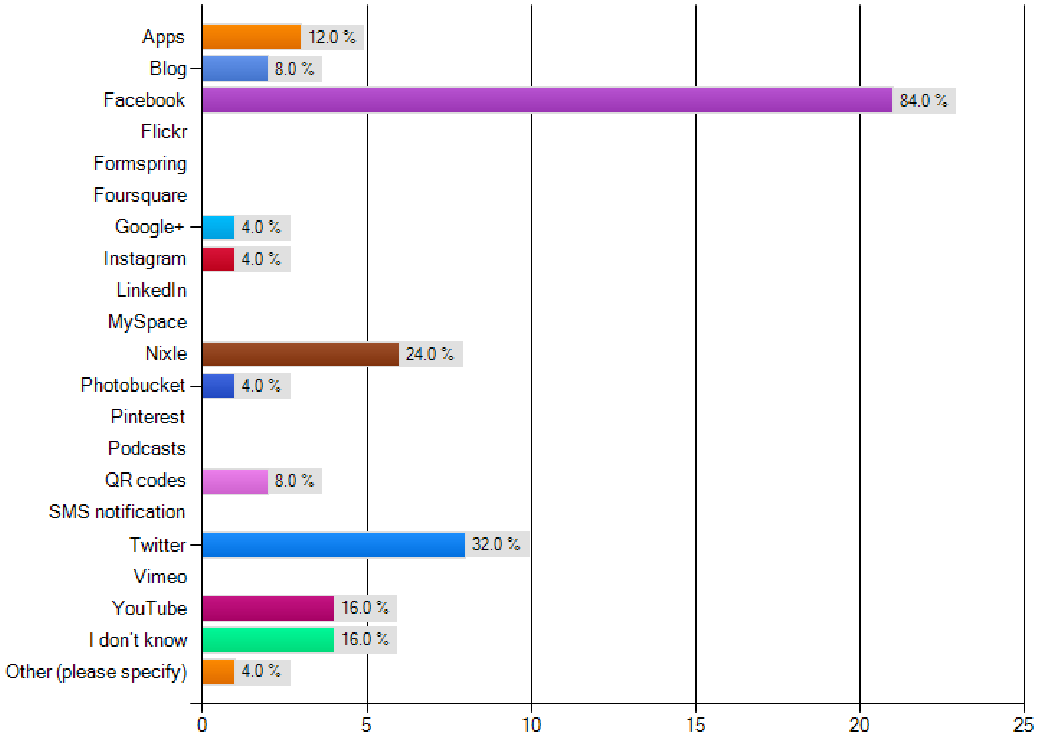


Questions for Agencies Not Using Social Media

Is your agency considering the adoption of social media?

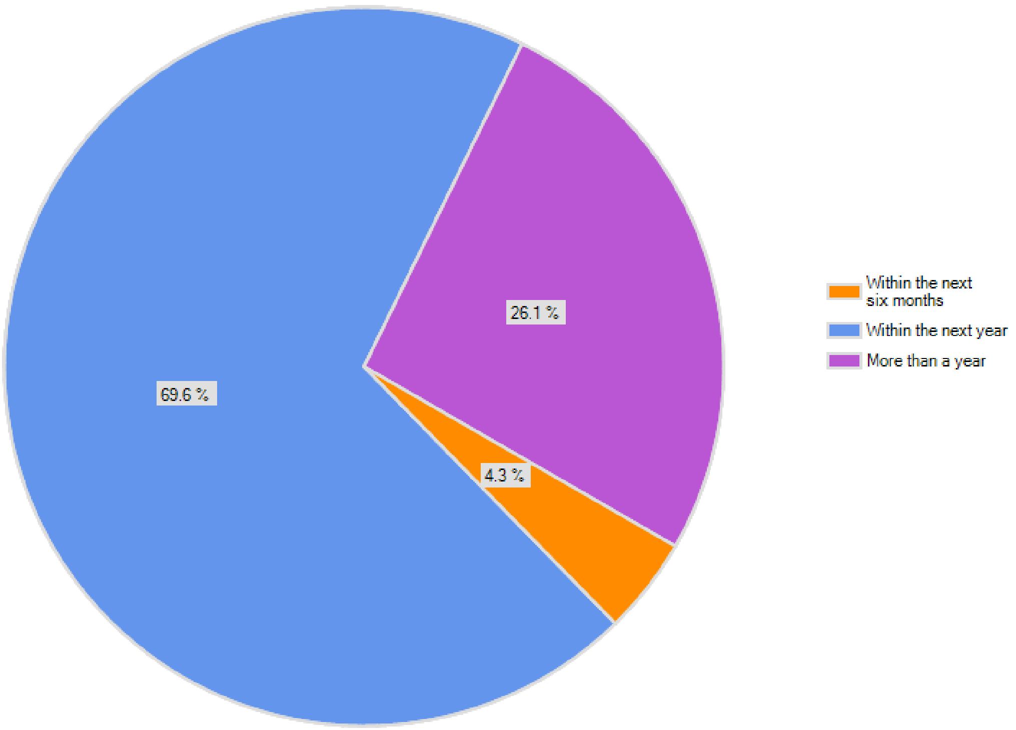


Which tools is your agency considering for adoption? (Select all that apply)

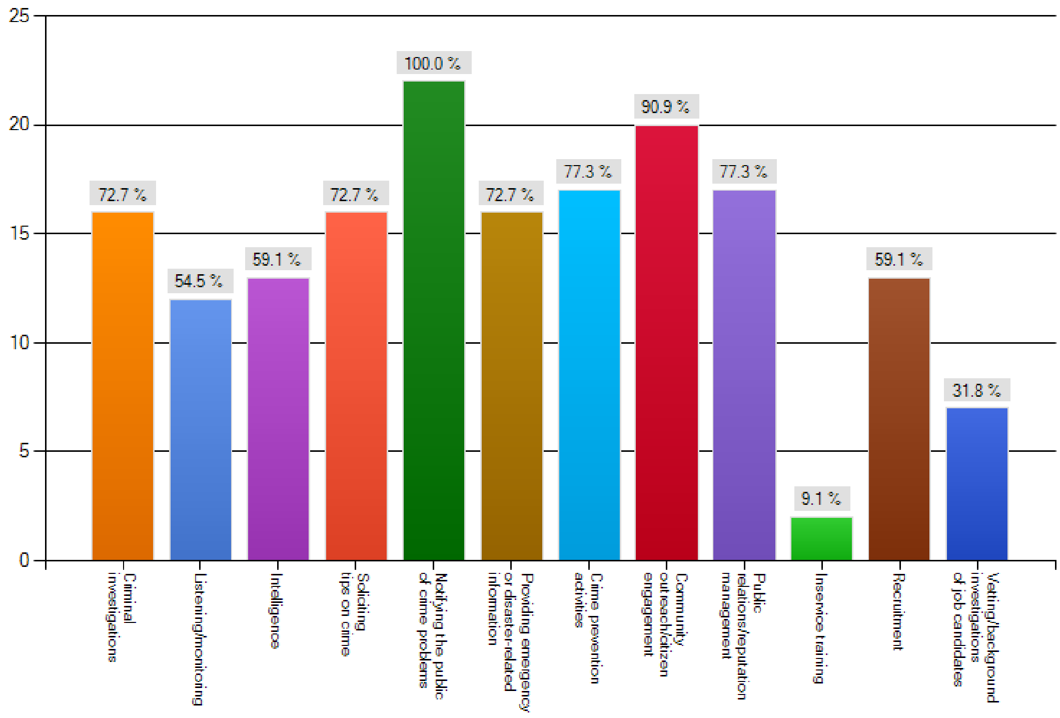


Questions for Agencies Not Using Social Media

What is your agency's anticipated time frame for establishing a social media presence?

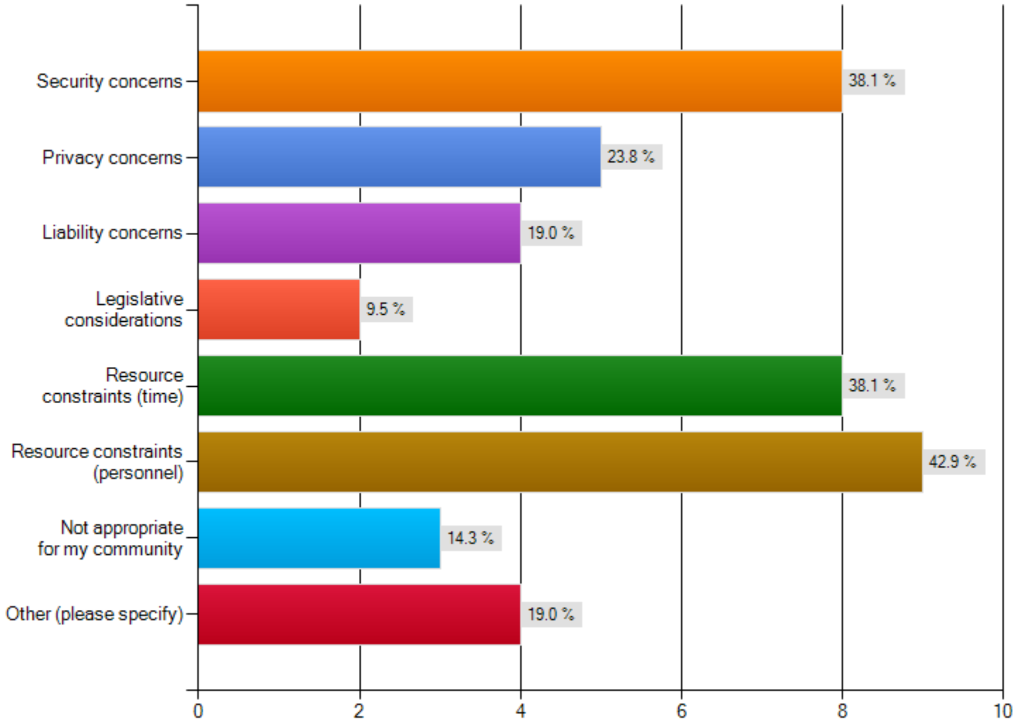


Which of the following activities does your agency anticipate using social media for? (Select all that apply)



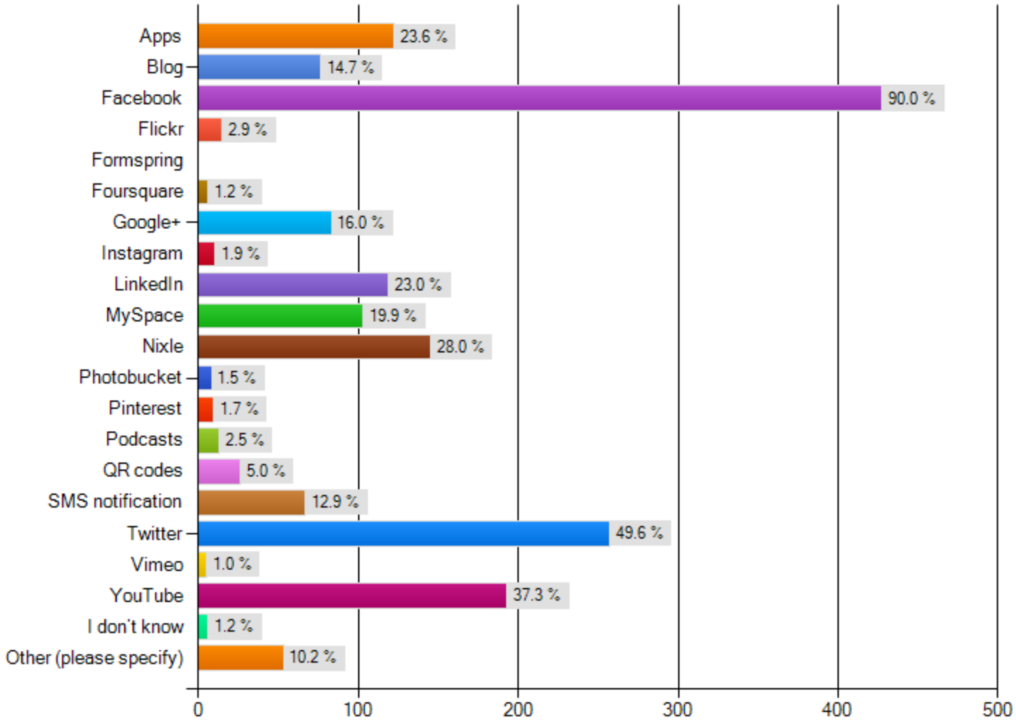
Questions for Agencies Not Using Social Media

What are the barriers to using social media in your agency? (Select all that apply)



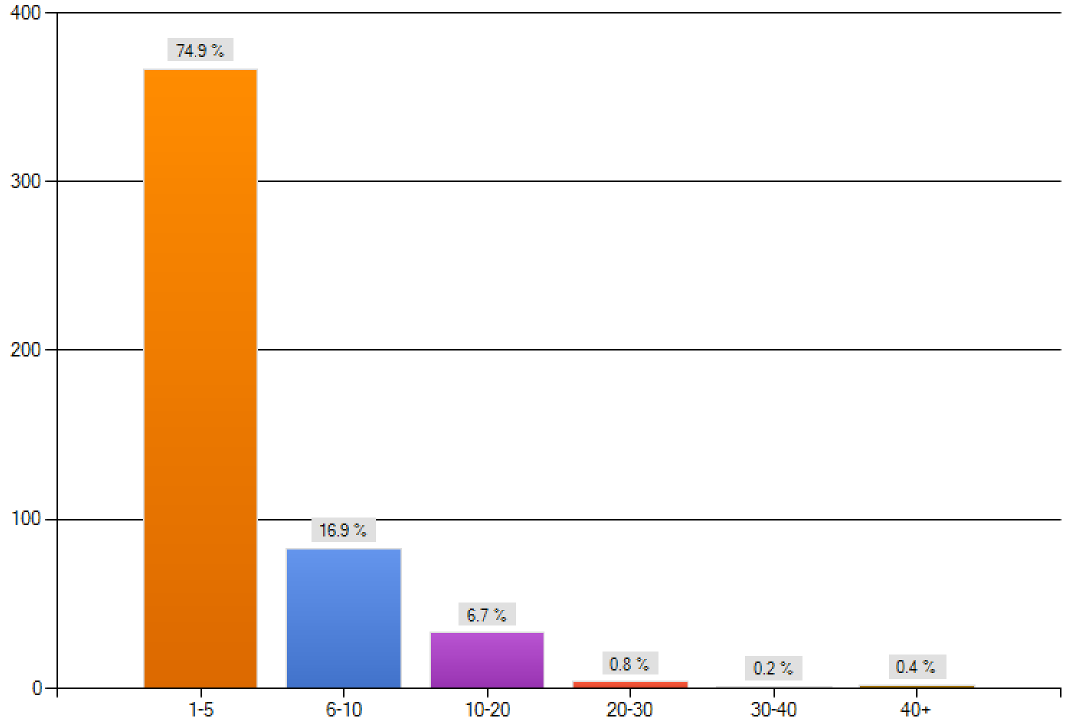
Questions for Agencies Using Social Media

What social media tools does your agency currently use? (Select all that apply)

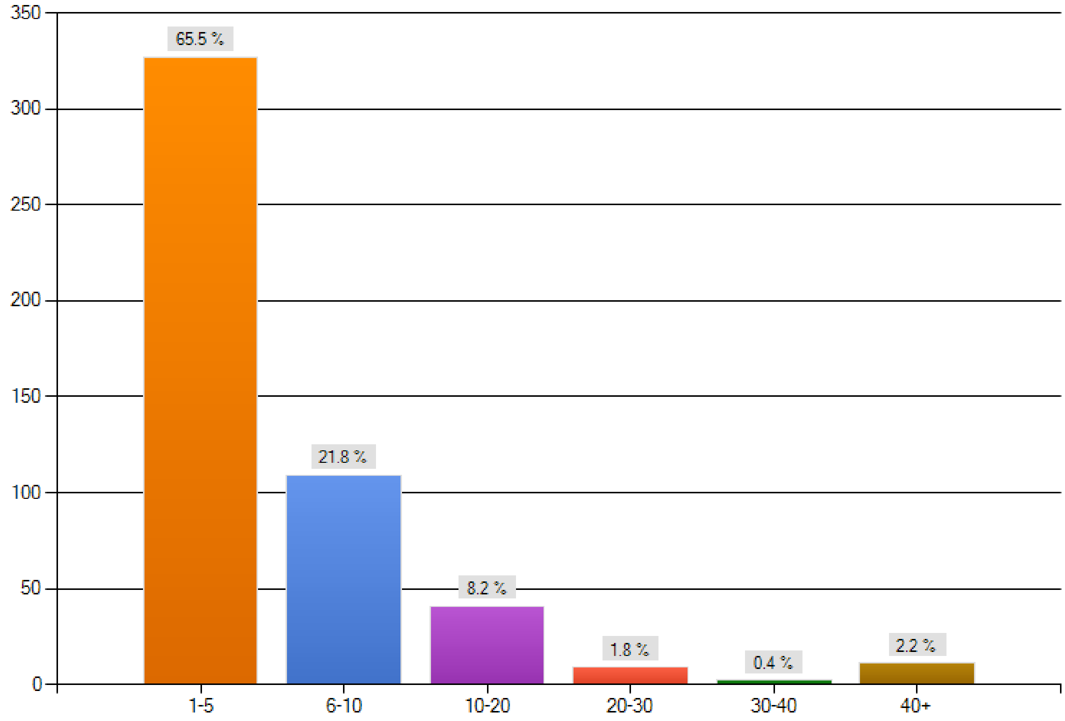


Questions for Agencies Using Social Media

How many hours are spent maintaining (developing and posting content, responding to comments, etc.) your agency's public social media presence on a weekly basis?

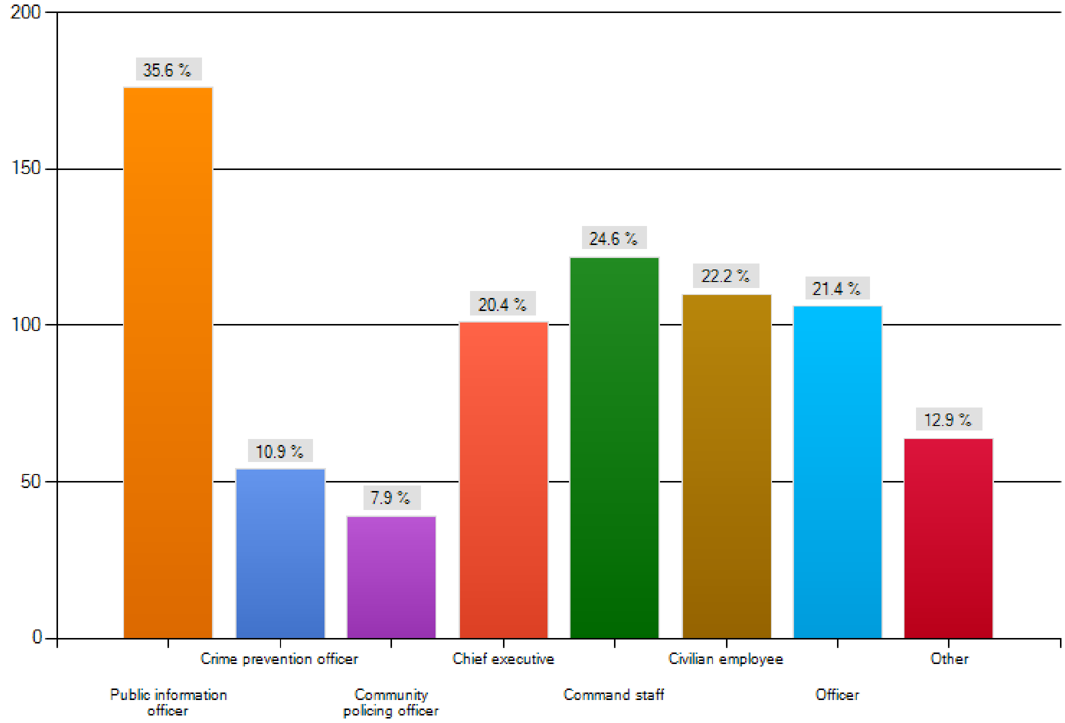


How many hours are spent using social media tools for intelligence or investigative purposes on a weekly basis?

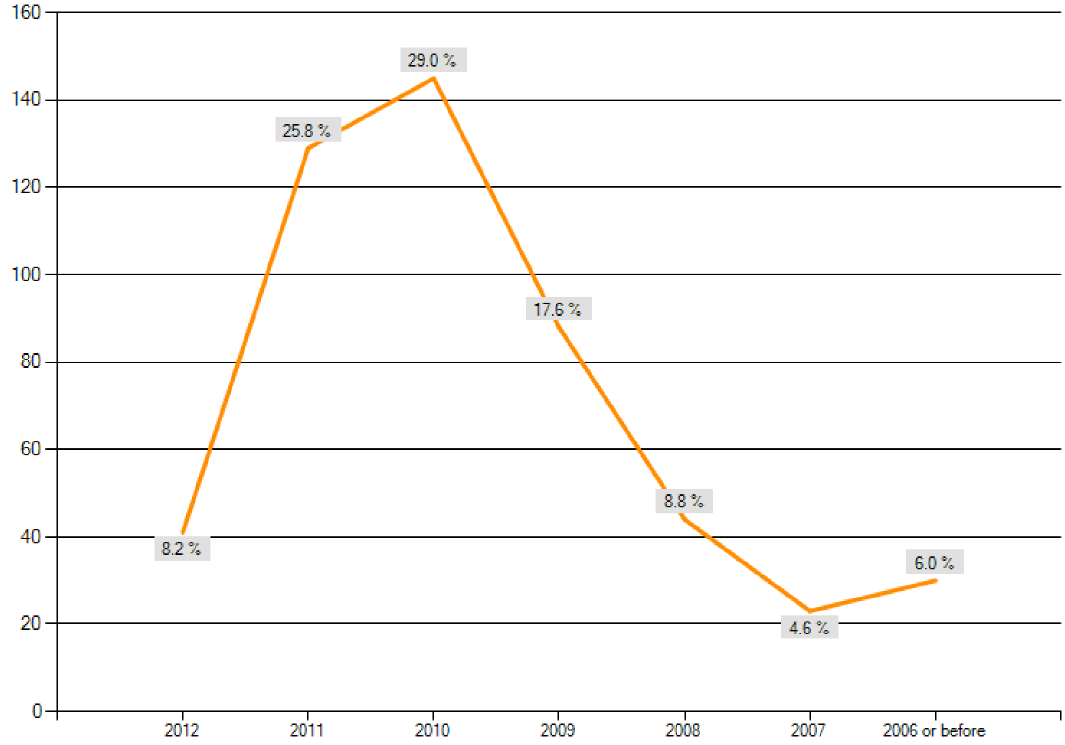


Questions for Agencies Using Social Media

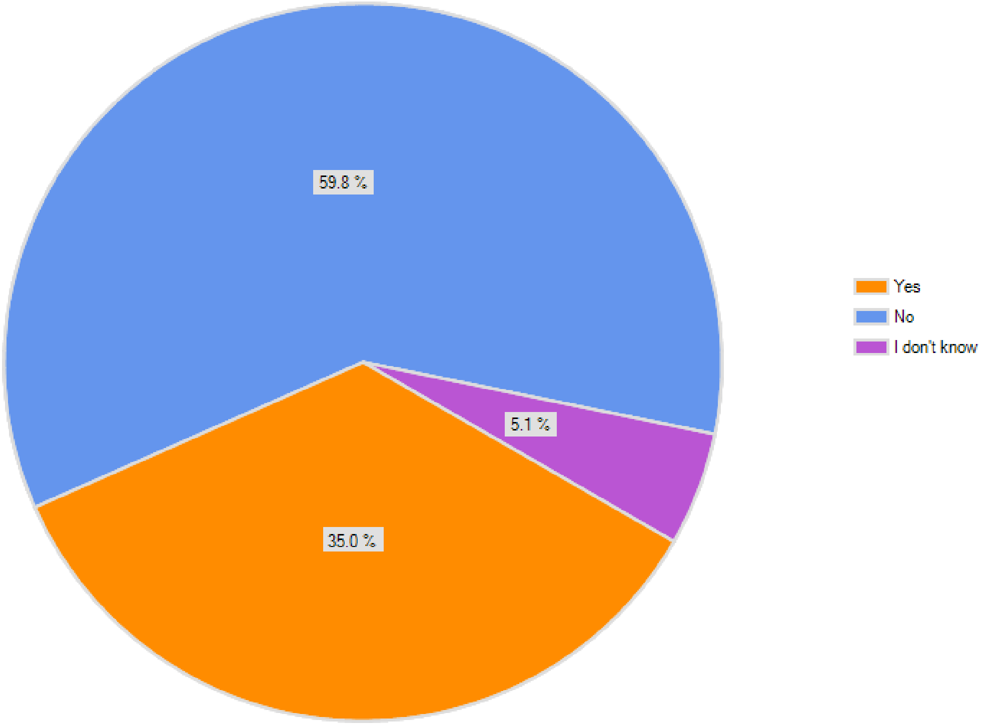
Who manages your agency's publicly-facing social media accounts on a day to day basis? (Select all that apply)



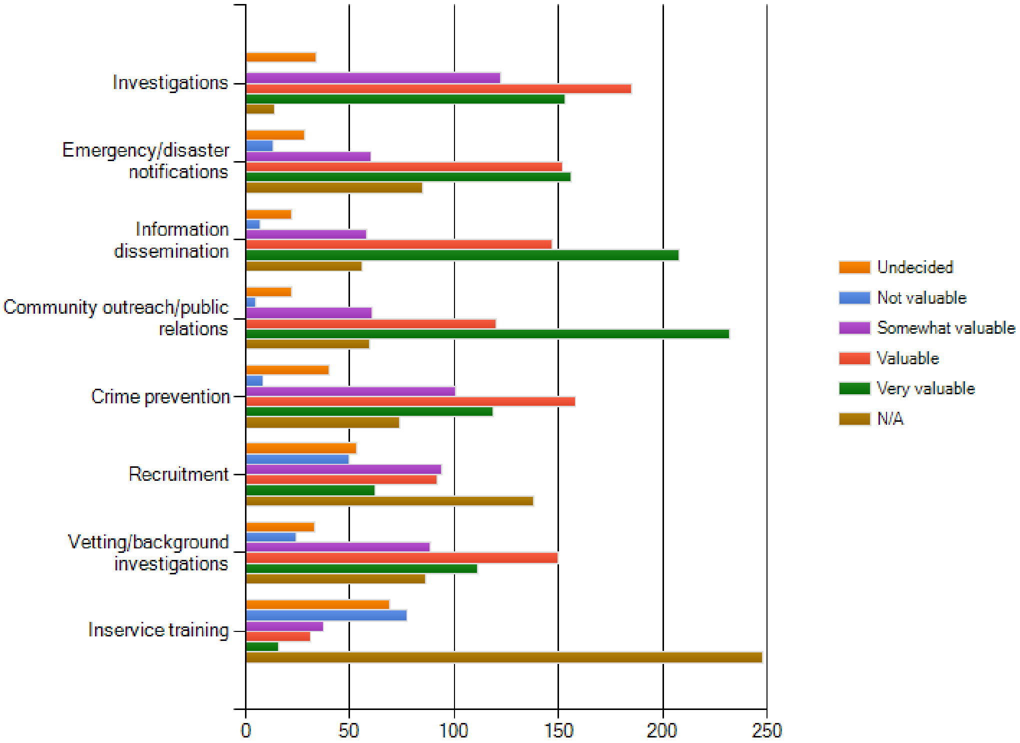
When did your agency start using social media?



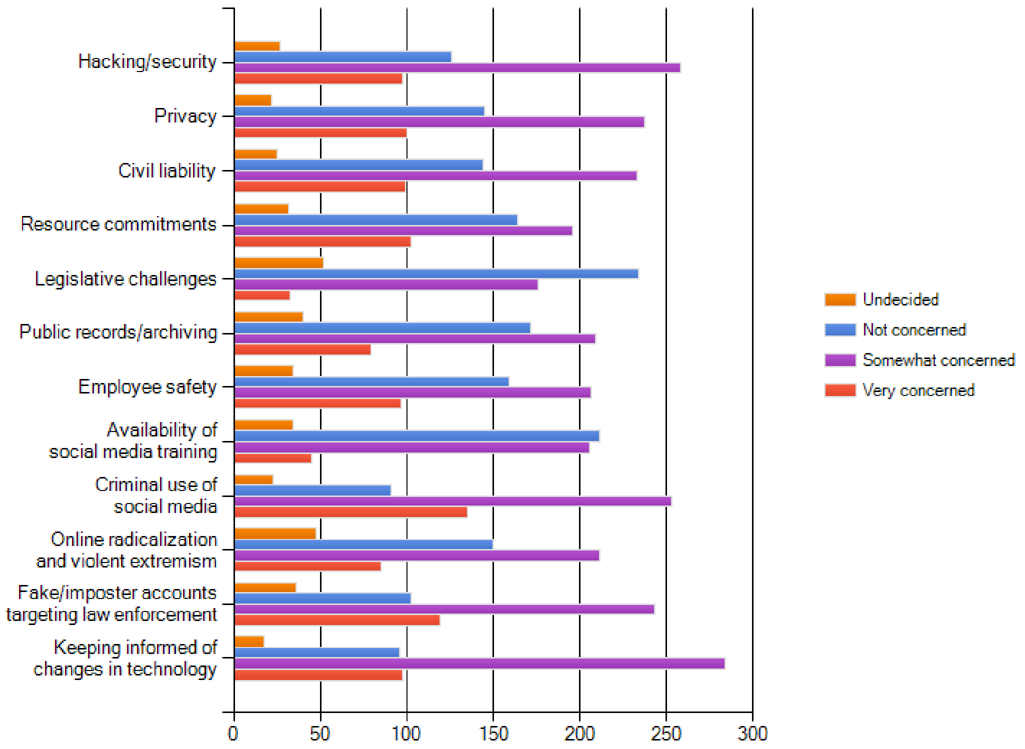
Has your agency identified goals and/or outcomes related to the use of social media?



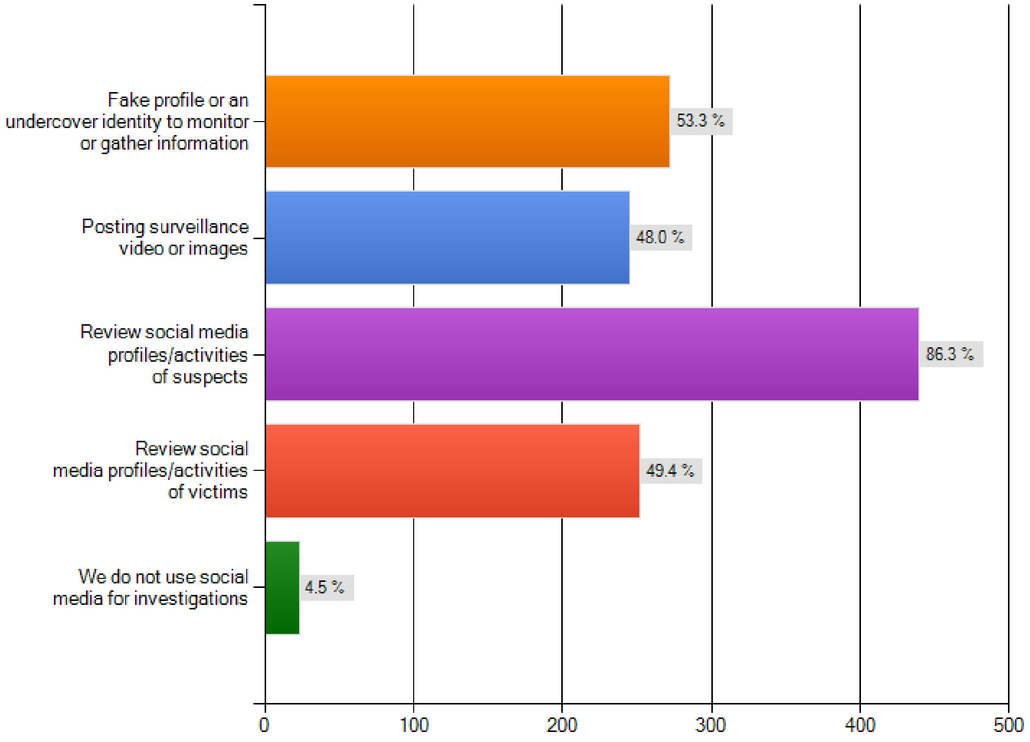
How valuable a tool is social media for your agency?



Please identify any concerns your agency has about social media.

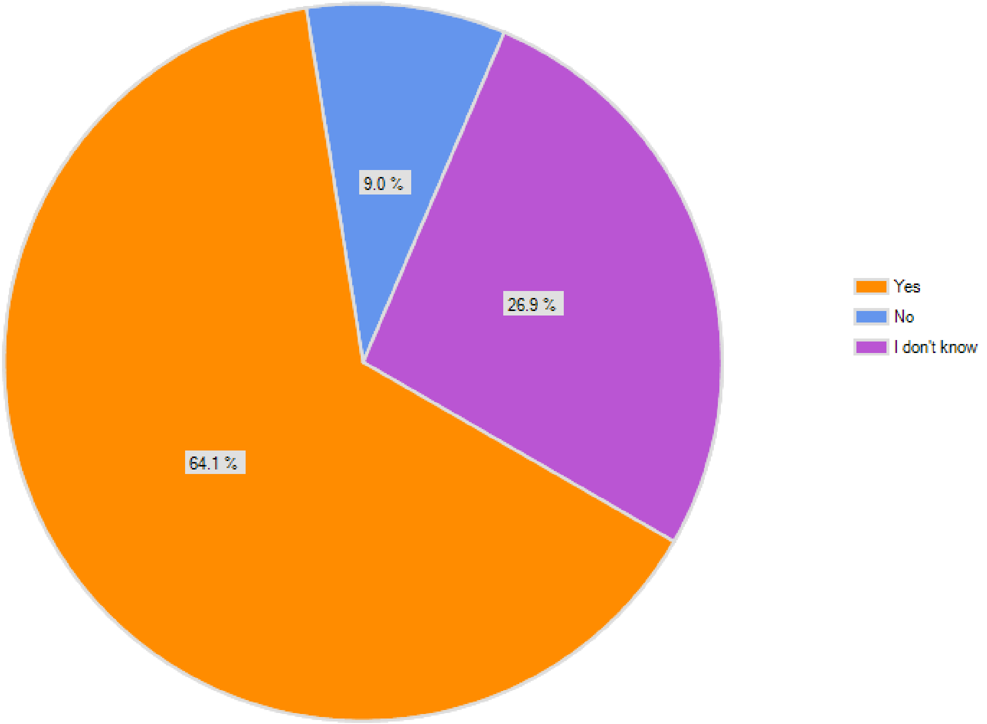


How does your agency use social media in investigations? (Select all that apply)

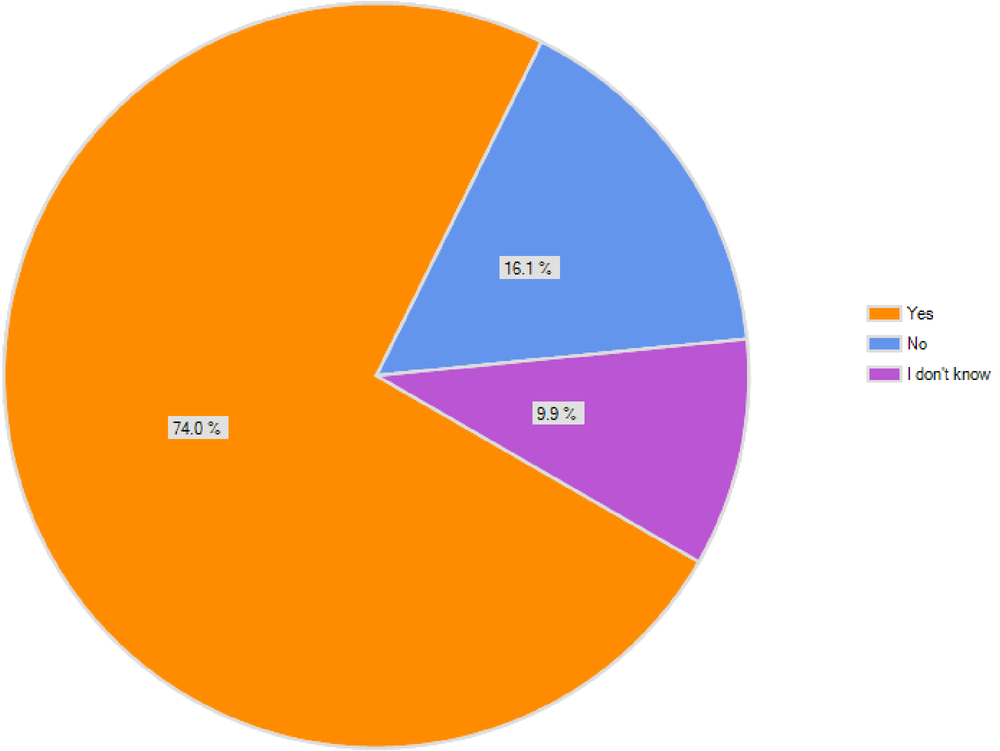


Questions for Agencies Using Social Media

Has social media improved police/community relations in your jurisdiction?

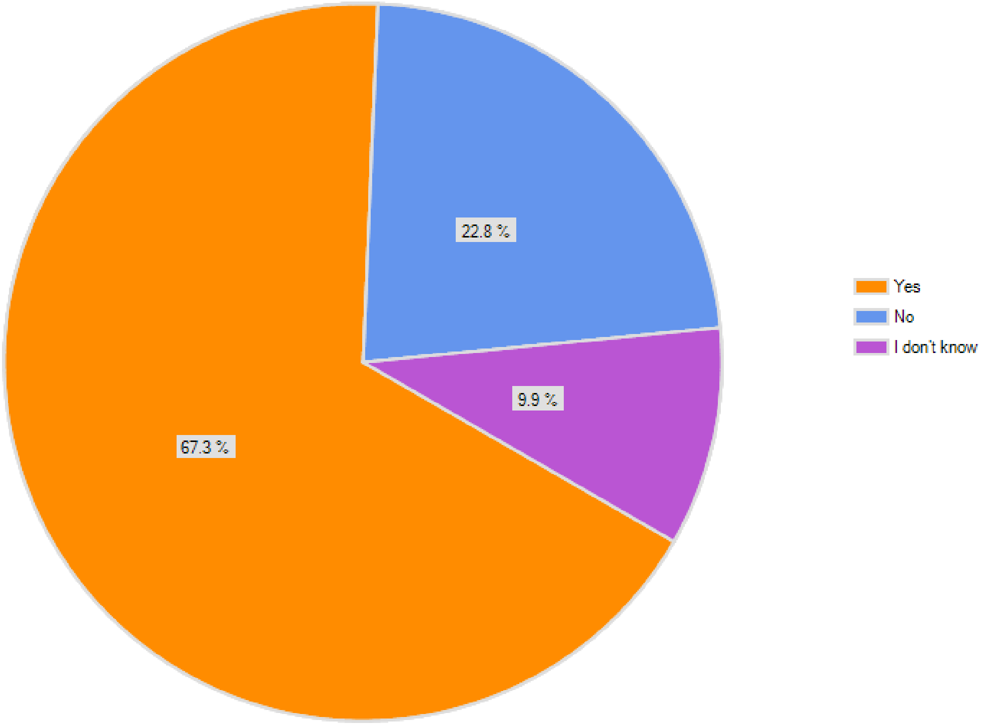


Has social media helped your agency solve crimes in your jurisdiction?

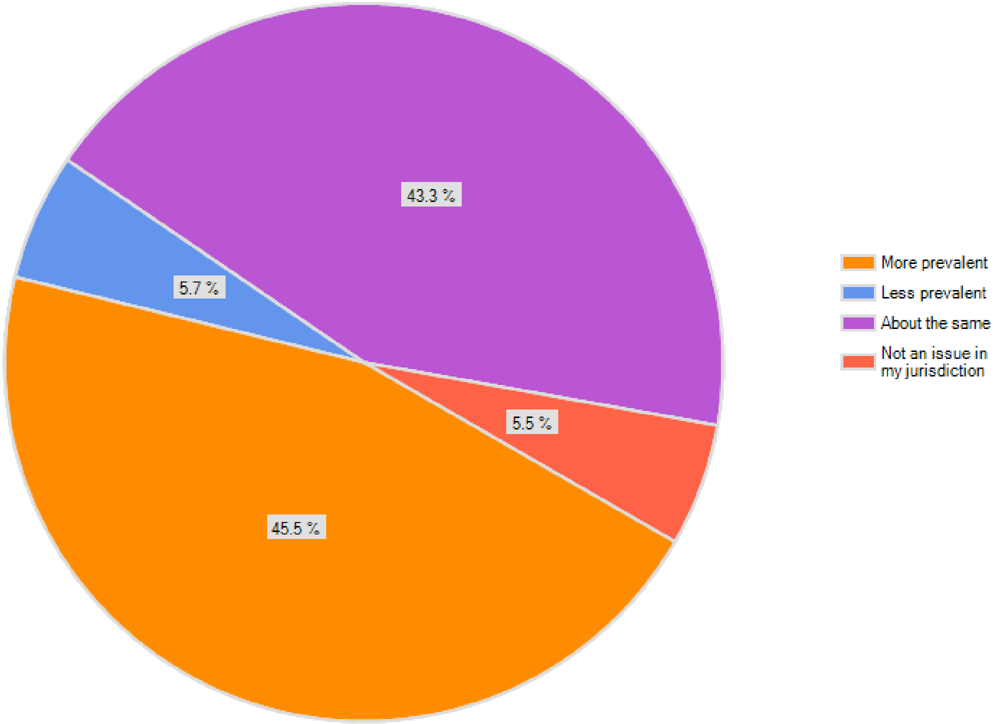


General Questions for All Respondents

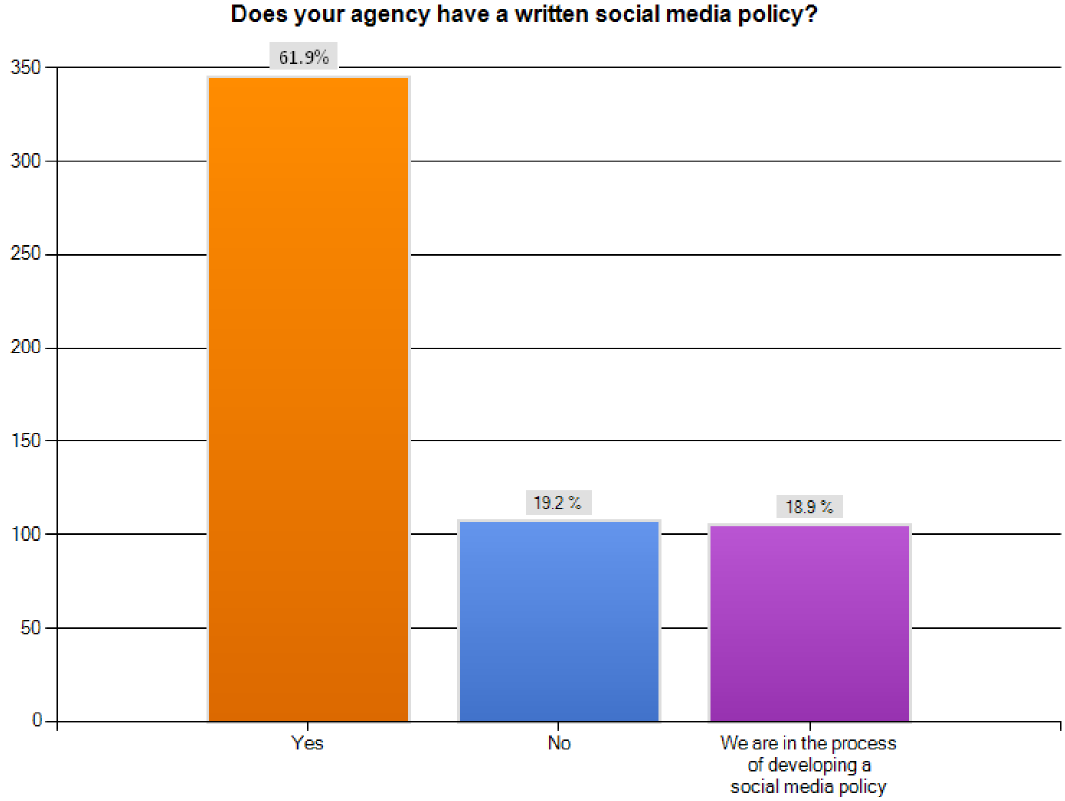
Does your unit of government, beyond your agency, use social media tools?

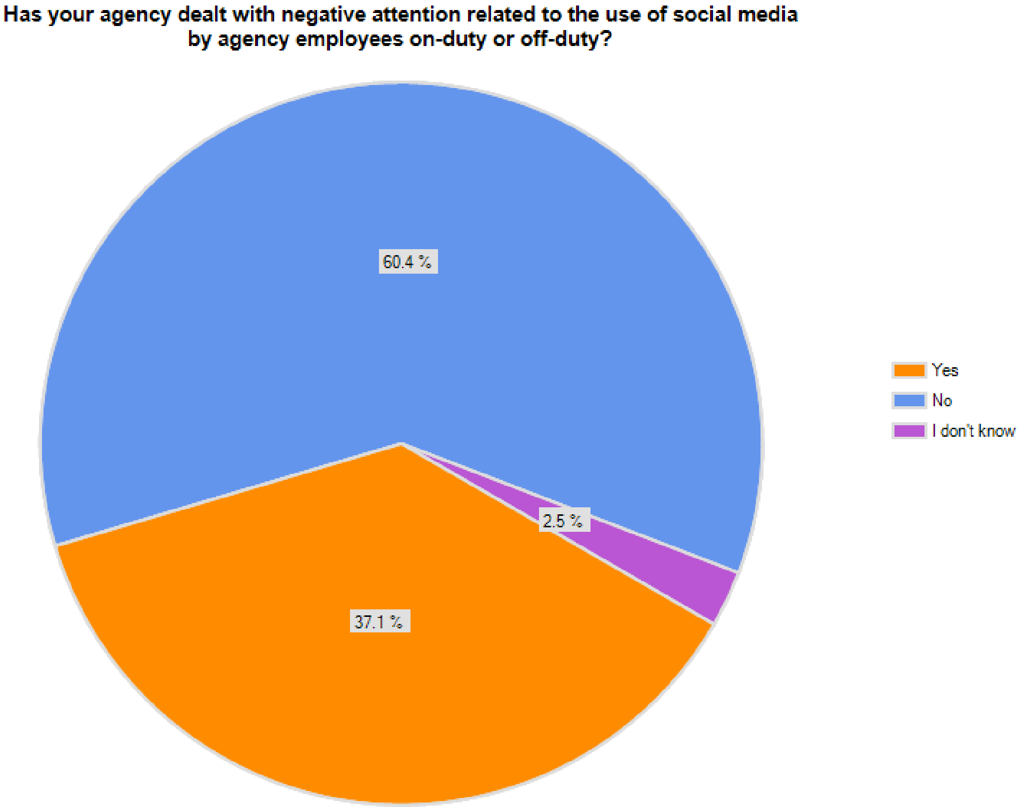


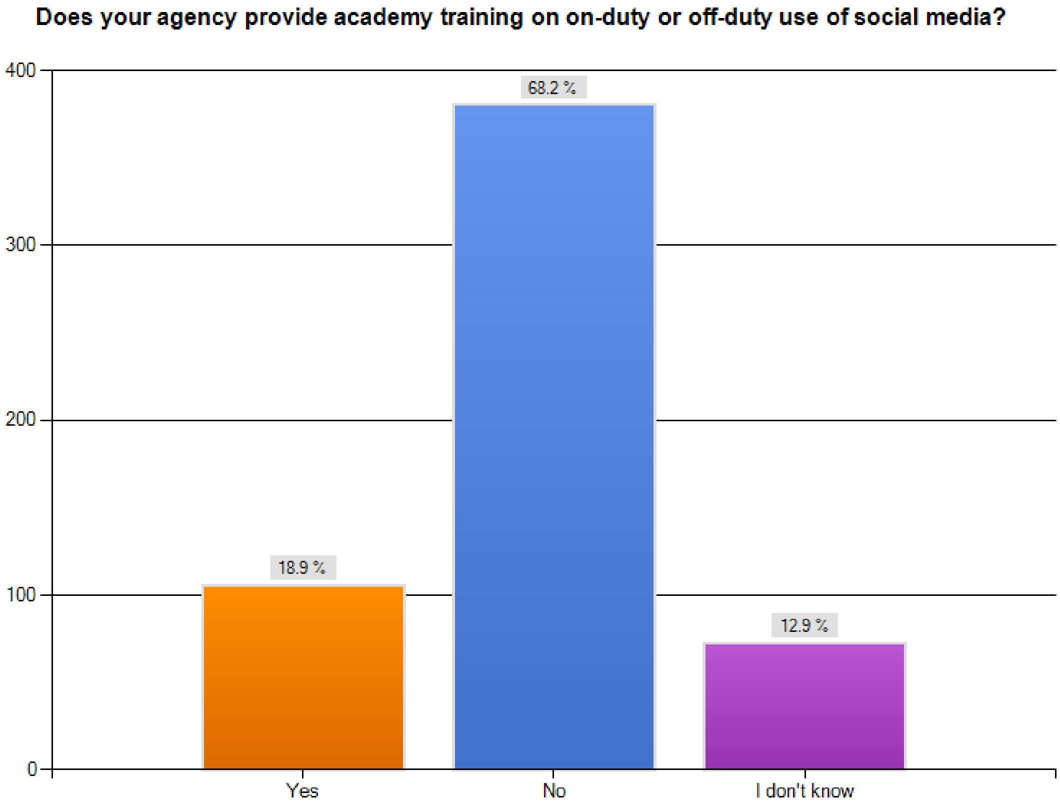
Compared to one year ago, concerns about employees' personal use of social media are:

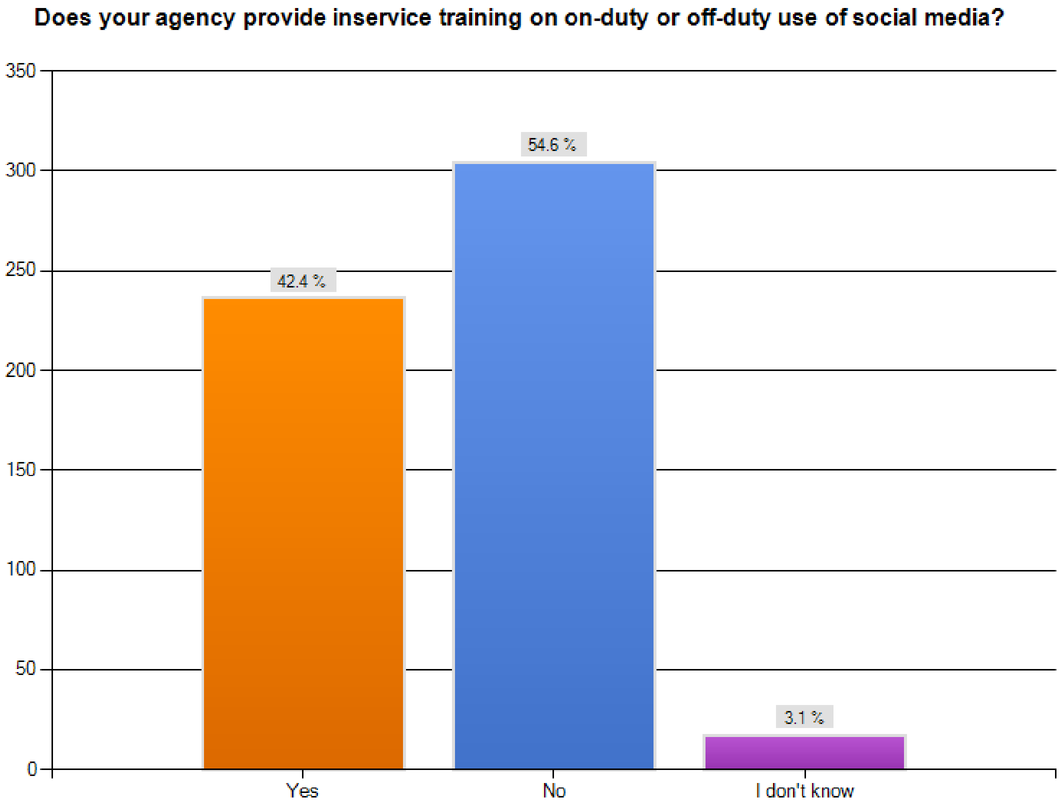


General Questions for All Respondents

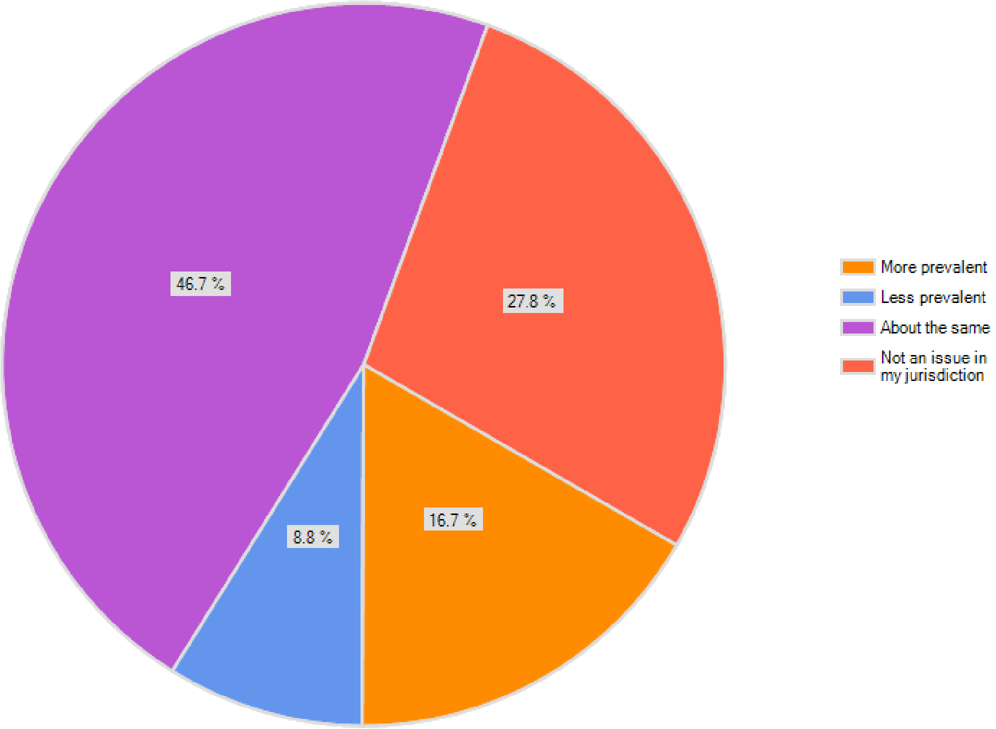




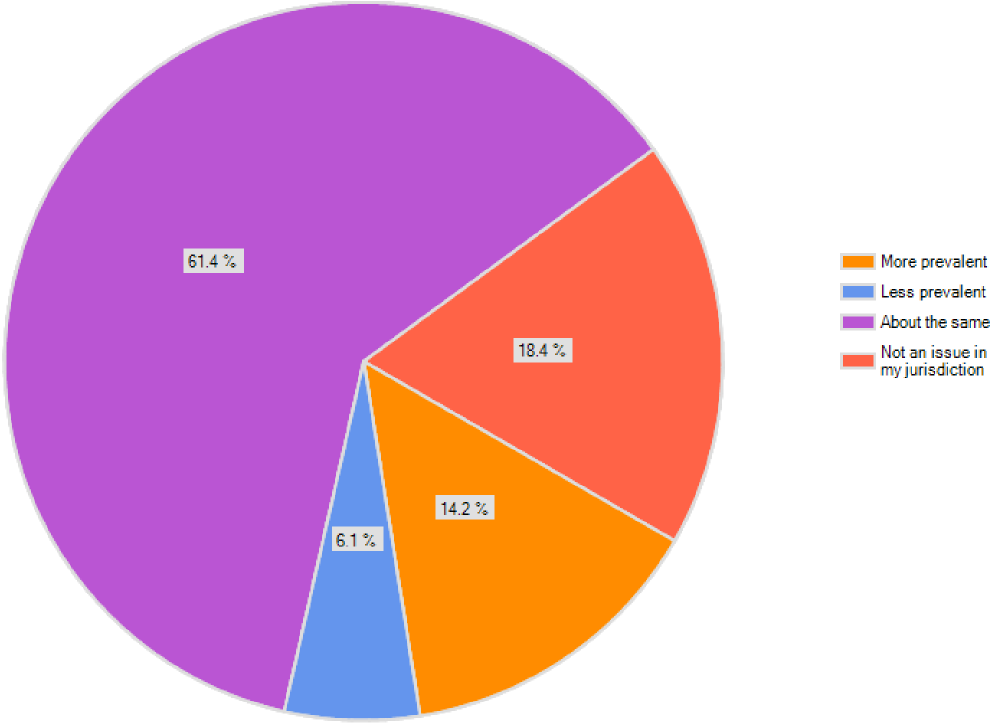

Does your agency provide academy training on on-duty or off-duty use of social media?
400
300
200
100
0
18.9 %
68.2 %
12.9 %
Yes
No
I don't know


Does your agency provide inservice training on on-duty or off-duty use of social media?
350
300
250
200
150
100
50
0
42.4 %
54.6 %
3.1 %
Yes
No
I don't know

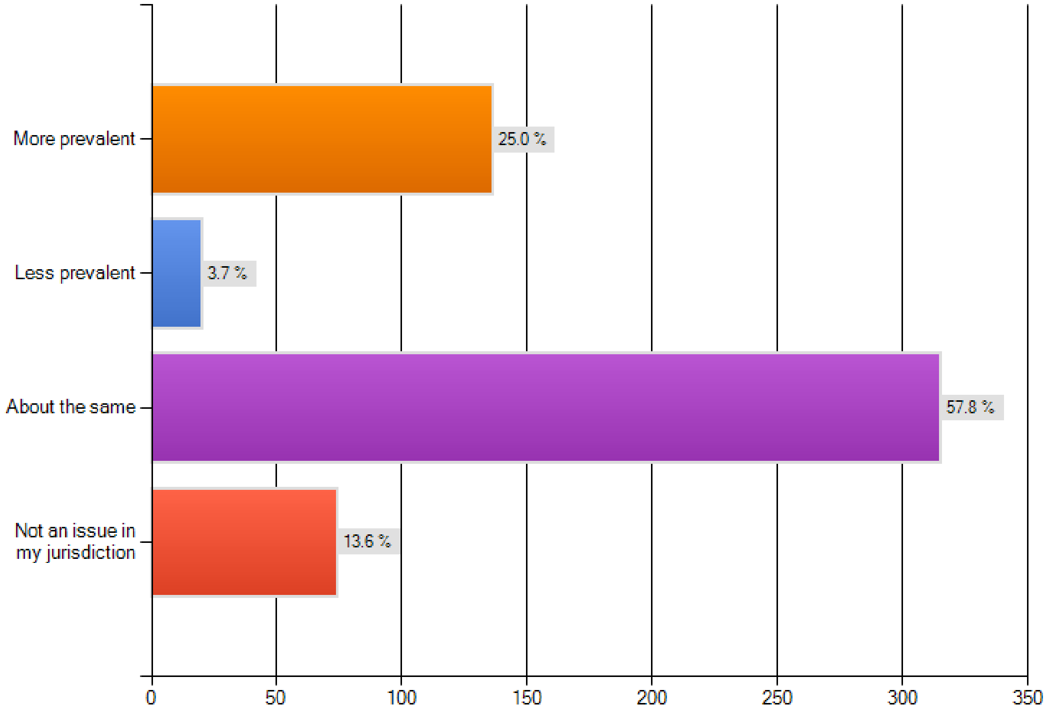
Compared to one year ago, complaints to my agency about "sexting" (the sharing of sexually explicit photos, primarily via cell phone) are:



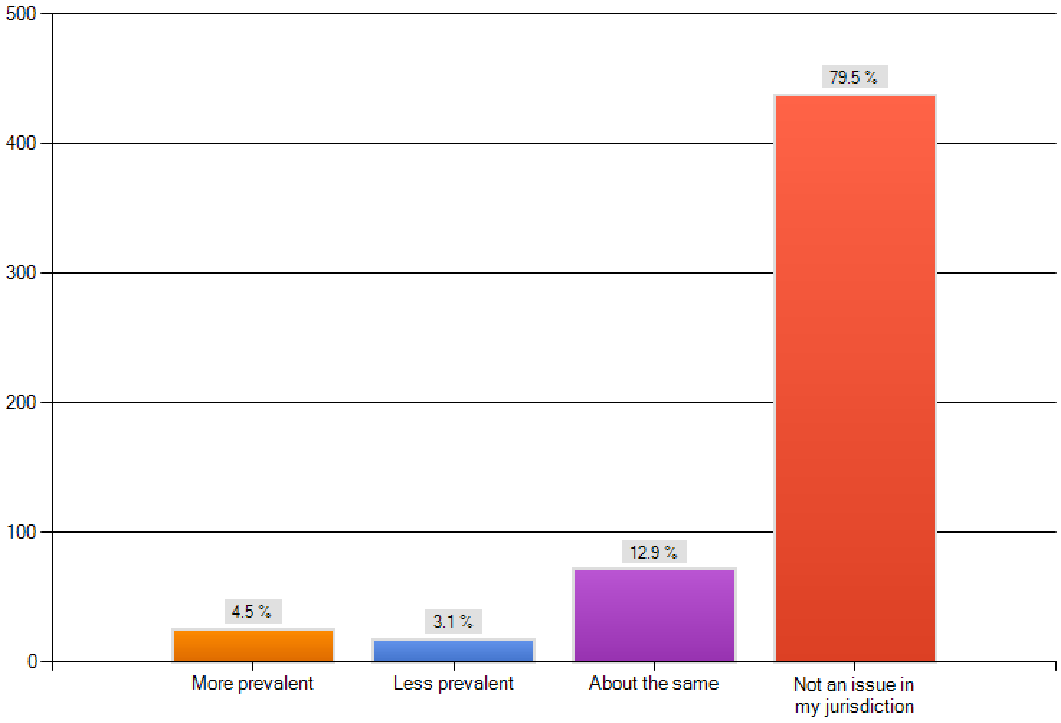
Compared to one year ago, complaints to my agency about online stalking are:



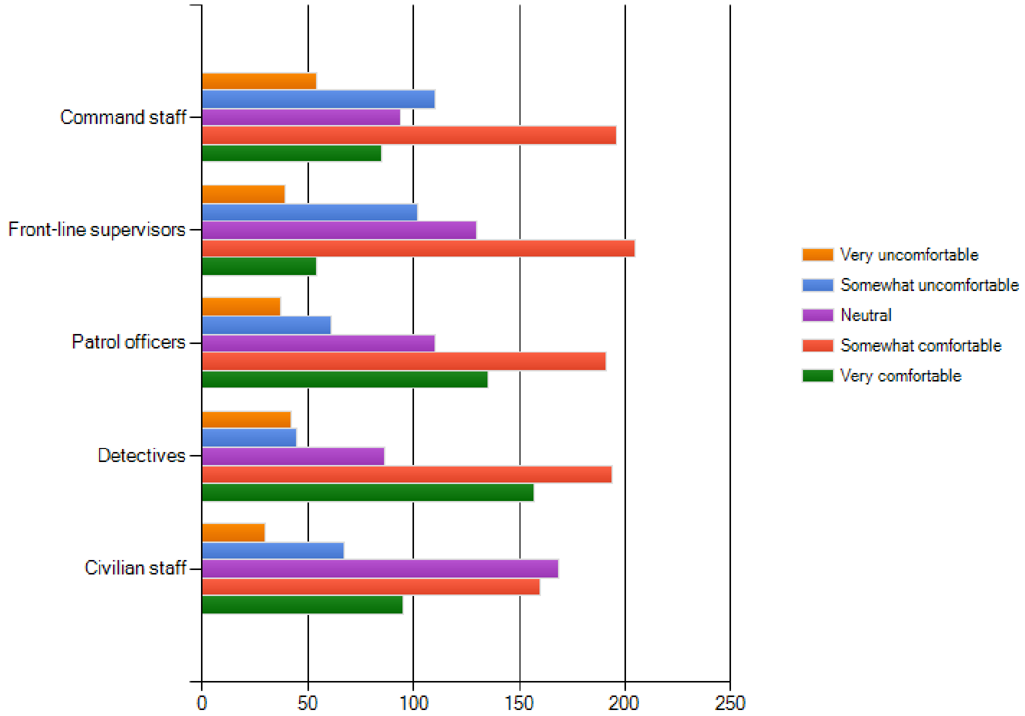
Compared to one year ago, complaints to my agency about online bullying/harassment are:



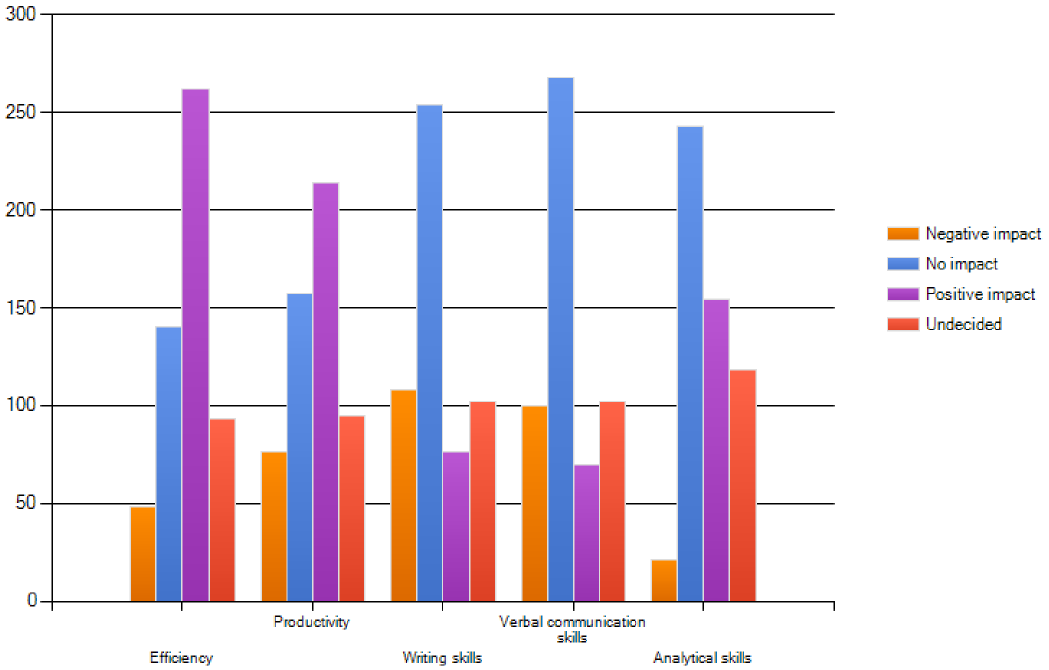
Compared to one year ago, complaints to my agency about flashmobs (large groups of individuals quickly mobilizing in a specific location) are:



Please rate the comfort level of your agency's staff with respect to the use of social media tools overall.



Social media has changed the way people learn, get information, do business, communicate, and interact with others. What impact has the proliferation of social media and reliance on related technology had on your agency's employees?



APPENDIX V

International Association of Chiefs of Police
2010 Annual Conference, Orlando

Social Networking in Law Enforcement

- First Amendment
  - Retaliation
  - Discovery of Identity of Anonymous Posters
  - Miscellaneous Issues
- Privacy
- Discovery
  - Attorney-Client Privilege Issues
  - Other Discovery Issues
- Civil Litigation, Miscellaneous
- Evidence
- Discipline cases
- Statutes
- Other Sources

Martha Stonebrook
Senior City Attorney
Salt Lake City, Utah
martha.stonebrook@slcgov.com

and

Rick Stubbs
Police Legal Advisor
Denver, Colorado
richard.stubbs@denvergov.org

First Amendment, Retaliation:

U.S. Supreme Court:

Garcetti v. Ceballos, 126 S. Ct. 1951 (2006)

1. When public employees make statements pursuant to their official duties, the employees are not speaking as citizens for First Amendment purposes and the Constitution does not insulate their communications from employer discipline.
2. The Court noted that supervisors must ensure that their employees' official communications are accurate, demonstrate sound judgment, and promote the employer's mission.
3. The Court also pointed out that exposing governmental inefficiency and misconduct is a matter of considerable significance; and public employers should, as a matter of good judgment, be receptive to constructive criticism offered by their employees.)

City of San Diego v. Roe, 125 S. Ct. 521 (2004)

1. Roe, a San Diego police officer, made a video of himself stripping off a police uniform and masturbating.
2. Under the user name "Code 3 stud@ aol.com," he sold the video on the adults-only section of eBay. He also sold police equipment including San Diego Police Department uniforms and men's underwear.
3. Roe's supervisor discovered Roe's activities while on eBay.
4. A SDPD investigation revealed that Roe had violated various SDPD policies including conduct prejudicial, outside employment, and immoral conduct.
5. SDPD ordered Roe to cease selling any sexually explicit materials or engaging in any similar behaviors via the Internet, U.S. mail, or any other medium available to the public.
6. SDPD subsequently learned that Roe only partially complied with the order.
7. Consequently, SDPD terminated Roe's employment.
8. The U.S. Supreme Court stated that a governmental employer may impose certain restrictions on the speech of its employees that would be unconstitutional if applied to the general public. On the other hand, when government employees speak or write on their own time on topics unrelated to their employment, the speech can have First Amendment protection,

absent some governmental justification far stronger than mere speculation in regulating it.

9. The Court stated that "public concern" is something that is a subject of legitimate news interest; that is, a subject of general interest and of value and concern to the public at the time of publication.

10. The Court easily concluded that Roe's expression did not qualify as a matter of public concern. The expression did not inform the public about any aspect of SDPD's functioning or operation.

11. The Court found that Roe took deliberate steps to link his videos and other wares to his police work, all in a way injurious to his employer, SDPD – through the use of a police uniform, a law enforcement reference in his website, the listing of the speaker as in the field of law enforcement, and the "debased parody of an officer performing indecent acts while in the course of official duties." All of these acts reflected negatively on SDPD and the professionalism of its officers.

12. Accordingly, the U.S. Supreme Court concluded that Roe's expression was not protected by the First Amendment and that his employer, SDPD, could take disciplinary action against Roe.

Rankin v. McPherson, 107 S. Ct. 2891 (1987)

1. First Amendment's free speech provision applies to probationary and at-will employees.

2. The fact that a statement is inappropriate or controversial is irrelevant to the question whether it deals with a matter of public concern.

3. If a statement is on a matter of public concern, the court must balance the employee's interest in making the statement against the interest of the state, as an employer, in promoting the efficiency of the public services it performs through its employees. The manner, time, place, and context of the statement are relevant to the balancing.

    - Pertinent considerations include whether the statement impairs discipline by superiors or harmony among co-workers, has a detrimental impact on close working relationships for which personal loyalty and confidence are necessary, or impedes the performance of the speaker's duties or interferes with the regular operation of the enterprise.

    - In weighing the state's interest in discharging an employee based on any claim that the content of her statement somehow undermines the mission of the public employer, some attention must be paid to the responsibilities of the employee within the agency. Where an employee serves no confidential, policymaking, or public contact role, the danger to the agency's successful functioning from that employee's private speech is minimal.

Connick v. Myers, 103 S. Ct. 1684 (1983)

1. When a public employee speaks not as a citizen upon matters of public concern but instead as an employee upon matters only of personal interest, absent the most unusual circumstances, a federal court is not the appropriate forum in which to review the wisdom of a personnel decision taken by a public agency allegedly in reaction to the employee's behavior.
2. Whether an employee's speech addresses a matter of public concern must be determined by the content, form, and context of a given statement, as revealed by the whole record. Not all matters that transpire within a government office are of public concern.
3. The First Amendment does not require a public office to be run as a roundtable for employee complaints over internal office affairs.

Courts other than the U.S. Supreme Court:

Hill v. City of Chicago, 2010 WL 3735723 (N.D. Ill. 2010)

1. Hill, an assistant commissioner of legal compliance with the City of Chicago, claimed that the city retaliated against her for complaining that she did not get a particular job due to illegal hiring practices.
2. Court determined Hill did not speak as an employee but as a private citizen.
3. Court further determined that whether the city's employment practices conformed to the law was a matter of public concern. The fact that an employee has a personal stake in the subject matter of the speech does not necessarily remove the speech from the scope of public concern.

Foley v. Town of Randolph, 598 F.3d 1 (1st Cir. 2010)

1. Fire Chief spoke at the scene of a fatal fire by stating that the fire department did not have sufficient staffing due to budget cuts.
2. Court found that Foley spoke on a matter of public concern because the budget and effectiveness of the fire department are important issues to the public.
3. However, Foley did not speak as a citizen, primarily due to the context of his speech – he was at the scene of a fire; he was in charge of the scene; he was in uniform; and, although not required to speak to the media, he was partially evaluated on media interaction.

4. In dicta court stated that Foley might be able to speak as citizen in a different forum – *e.g.*, at a town meeting, in a letter to the editor, or even in a statement to the media under different circumstances.

Desrochers v. City of San Bernandino, 572 F.3d 703 (9th Cir. 2009)

1. Two police sergeants claimed one received an unfavorable assignment and the other a 15-day suspension due to filing a grievance in which they criticized two lieutenants who supervised them.
2. Court held the speech was not on a matter of public concern and, therefore, not protected by the First Amendment. While the plaintiffs tried to characterize their speech as addressing competency, efficiency, and morale, the court found the speech focused on one lieutenant as a bully. Court said a reference to government functioning does not create a matter of public concern; court looks to what was actually said in the speech at issue rather than the speaker's subsequent characterizations of his/her speech. Because the speech was contained in an internal grievance, it did not reach a large public audience.

Ranck v. Rundle, 2009 WL 1684645 (S.D. Fla. 2009)

1. Plaintiff was an attorney in a prosecutor's office
2. He investigated a police shooting and determined there were possible problems with the shooting; he conveyed that information to the lead detective on the investigation and his superiors (in a memo).
3. His superiors decided to remove him from the investigation
4. After obtaining via a public records request a copy of the memo and other internal documents, Ranck posted them on a blog he created and sent a link accessing those postings to a blog used by criminal defense lawyers.
5. He was suspended without pay for 30 days for publicly releasing information about an ongoing police shooting investigation; posting offensive comments about his colleagues; inflicting harm to the integrity, reputation, and well-being of the prosecutors' office; exhibiting a lack of candor as to approval for payment of expert witness fees in a separate matter; and in-court misconduct in a separate matter.
6. Court determined that plaintiff wrote the memo pursuant to his official duties but that he posted the memo as a private citizen whose speech was intended to raise concerns about the handling of the shooting investigation; because the content of the speech related to whistle-blowing, because it was communicated to the public at large, and because his motivation was to

raise concerns about the investigation, the speech was on a mater of public concern.

7. The court found that plaintiff’s First Amendment interests in the speech outweighed the state’s interest in promoting the efficiency of its services.

8. However, the court concluded that the agency had legitimate reasons for suspending the plaintiff and, as a result, there was a legitimate issue as to whether he was disciplined due to his speech. Summary judgment granted for employer.

Herdegen v. City of Los Angeles, 2008 WL 224011 (Cal. Ct. App. 2008)

1. Police department issued to recruit officers a document discussing a specific requirement to become a police officer and instructed them to sign the document.

2. Plaintiff, one of the recruits, allegedly made comments to some of the other recruits that they should not sign a document they did not understand, that they should contact the union, and that the city was looking out for its own interests rather than those of the officers.

3. Court determined that the speech was not on a matter of public concern because officer did not comment substantively on the policy. The fact that the speech referred to a union did not automatically mean the speech merited First Amendment protection.

Nixon v. City of Houston, 511 F.3d 494 (5th Cir. 2007)

1. City police officer wrote articles for a local magazine in which he identified himself as a police officer; discussed police-related duties and activities; and made caustic, offensive, and disrespectful comments toward certain minority groups, women, and the homeless. Also, without authorization he went to the scene of a highly-publicized, high speed police pursuit; asked a supervisor if he could make a statement to the media; and, when the supervisor’s only response was to laugh, he made a statement to the media in which he criticized HPD’s decision to disengage the pursuit and stated he was embarrassed to be an HPD officer because the department did not stop fleeing felons. The next day, he made statements on numerous radio talk shows and to TV interviewers criticizing DPD and its pursuit policy.

2. As a result of these statements, DPD terminated Nixon’s employment.

3. The Fifth Circuit found that Nixon (who was on-duty, in uniform, and requested permission to make the statements) made his statements at the scene of the accident during the course of performing his job and not as a citizen despite the fact that he was not authorized to make the statements.

4. With respect to Nixon's statements to radio talk shows and TV interviewers: They are more like citizen speech. However, Nixon's interests in making the statements are outweighed by HPD's interests in maintaining discipline and order among employees and in promoting and maintaining public confidence in HPD. Because police departments function as paramilitary organizations charged with maintaining public safety and order, they are given more latitude in their decisions regarding discipline and personnel regulations than an ordinary government employer.

5. With respect to Nixon's comments regarding minorities, women, and the homeless: The exposure to Houston's minority community and the caustic nature of the comments could negatively impact HPD's relations with the minority community. Those relations are important because citizens need to respect law enforcement officers, often provide valuable information regarding crimes, serve as witnesses, and provide financial support.

Dible v. City of Chandler, 515 F.3d 918 (9th Cir. 2008)

1. Chandler Police Officer Ronald Dible posted on a website: (a) photographs of his wife, Megan Dible, in various sexual poses and sexual activities with Ronald Dible, another woman, and inanimate objects; and (b) a videotape of Megan masturbating that had been filmed by Ronald. Viewers had to pay see those photographs and videotape. The website also offered for sale a CD-ROM with content similar to the photographs and videotape. The home page to the website featured partially nude pictures of Megan to entice viewers to pay to see the photographs and videotape. The Dibles promoted their website at meetings and on other websites.

2. The Dibles did not intend to express any kind of message on the website; they intended only to make money.

3. Because Ronald Dible believed that his role with the website was not compatible with his position as a police officer, he attempted to conceal its existence from Chandler P.D. officials.

4. However, CPD eventually learned of the website and terminated Ronald's employment.

5. Before CPD dismissed Dible, the press learned of the website and reported on it in an unflattering manner. That publicity resulted in members of the public showing disrespect to CPD officers, potential police recruits asking questions about the website, possible problems in recruiting female officers, and diminished officer morale.

6. In evaluating Ronald's First Amendment free speech claim, the Ninth Circuit applied the analysis enunciated by the U. S. Supreme Court in *City of San Diego v. Roe*.

7. Ronald's attempt to separate the website from his position as a police officer did not aid his First Amendment claim because CPD officers and the public eventually learned of the website, causing injury to CPD.

8. The Ninth Circuit noted that the interest of the city in maintaining the effective and efficient operation of its police department is particularly strong. Police departments and the persons who work for them are engaged in a dangerous calling and have significant powers. The public expects officers to behave with a high level of propriety and is outraged when they do not. The law and officers safety demands that officers be given a degree of respect and the "sleazy" activities of the Dibles undermined that respect.

9. The court concluded that Ronald's First Amendment free speech claim must fail.

10. The Ninth Circuit also rejected Ronald's First Amendment right of privacy claim. The court pointed out that, while Megan engaged in "intimate" activities, those activities were not intimate in the sense that the Dibles made them available to the public for the price of admission to the website.

11. With respect to Ronald's First Amendment freedom of association claim: The court held that Ronald did not have a right to participate in the activities and to avoid city discipline.

See v. City of Elyria, 502 F.3d 484 (6th Cir. 2007) (Officer's claim for First Amendment retaliation due to being discharged survived defendant's motion for summary judgment where officer reported the following issues to the FBI: (a) concerns about the grand jury procedures used by the department; (b) policies prohibiting officers from speaking to the press; (c) the police chief's allegedly allowing an officer to work unnecessary overtime; and (d) plaintiff's belief that the police chief had manipulated the results of an investigation in order to protect a public official. The court concluded that issues these are matters of public concern which demand strong First Amendment protection.)

Gonzales v. City of Calexico, 2007 WL 2001180 (S.D. Cal. 2007) (good discussion of why the federal district court rejected defendant's summary judgment motion where plaintiff probationary police officer engaged in limited participation in protest related to fellow officers' desire to maintain possession of certain rifles and defendant's dismissal of plaintiff subsequent to the protest; the type of personnel matters that are unprotected under the public concern test are employment grievances in which the employee is complaining about his/her own job treatment and no about personnel matters pertaining to other persons)

Golt v. City of Los Angeles, 2006 WL 3804367(9th Cir. 2006) (Plaintiff Golt's First Amendment claim failed because she did not speak on matters of public concern: (a) her distribution of cards requesting that the police chief not attend funerals of LAPD officers killed in the line of duty pertained only to an internal workplace grievance and did not inform the public about any aspect of LAPD's functioning or operations or reveal failure to discharge governmental responsibilities, illegal conduct, breach of the public trust, or misuse of public funds; and (b) her testimony at a disciplinary hearing concerned only a specific issue of sexual harassment and did not contribute to the resolution of an administrative proceeding in which discrimination or other significant government misconduct is at issue.)

Miller v. Jones, 444 F.3d 929 (7th Cir. 2006) (plaintiff stated First Amendment claim sufficient to withstand summary judgment motion where speech that opposed a proposed merger between police program and another organization touched on a matter of public concern)

Wallace v. Suffolk Cty. Police Dep't, 396 F. Supp. 2d 251 (E.D.N.Y. 2005) (plaintiff police officer's comments were on matters of public concern: he alleged that the police department did not have proper training protocols or equipment to ensure the safety of its officers or the public; also, plaintiff's claim that his injuries were purposefully omitted from his retirement application in order to penalize him for his protected speech was sufficient, at the summary judgment stage, to establish an adverse employment action (which is a material adverse change in the terms and conditions of employment))

Signore v. City of Montgomery, 354 F. Supp. 2d 1290 (M.D. Ala. 2005) (police officer was not speaking on a matter of public concern when he assumed a media representative already knew about a police vehicle's being stolen and his speech to the media representative was intended, at least in part, to obtain information for the officer; furthermore, the officer's disclosure of information about an on-going investigation can cause the *Pickering* balancing to weigh in favor of a police department)

First Amendment, Discovery of Identity of Anonymous Posters:

Juzwiak v. Doe, 2 A.3d 428 (N.J. Superior Ct., App. Div. 2010)

1. Plaintiff high school teacher received e-mails containing the following statements: (1) "Hopefully, you will be gone permanently. We are all praying for that. [signed] Josh." (2) "You don't deserve to teach anymore.

I will make it my life's work to ensure that wherever you look for work, they know what you have done."

2. A third e-mail that was sent to plaintiff and community members contained the following statement: "We can not continue to allow the children of this school system nor the parent to be subjected to his evil ways."

3. Plaintiff did not know who was responsible for authoring and sending the e-mails.

4. Plaintiff filed a complaint in New Jersey state court against a John/Jane Doe defendant.

5. Plaintiff served a subpoena on Yahoo!, the internet service provider, seeking the author's identity.

6. Yahoo! notified the subscriber of the subpoena, who moved to quash the subpoena.

7. The appellate court noted that the right to speak anonymously is protected by the First Amendment and derives from the principle that, to ensure a vibrant marketplace of ideas, some speakers must be allowed to withhold their identities to protect themselves from harassment and persecution. But the right to speak anonymously is not absolute. Plaintiffs have the right to seek redress for legally cognizable speech and speakers cannot escape liability simply by publishing anonymously.

8. New Jersey law on the right of plaintiffs to obtain the identity of anonymous speakers is as follows: First, the plaintiff must attempt to directly contact the anonymous poster. Second, in the complaint the plaintiff must set forth the exact statements made by the poster. Third, the court must carefully review the complaint and all information provided to determine whether the plaintiff has set forth a *prima facie* cause of action. Fourth, the court must balance the defendant's First Amendment right of anonymous free speech against the strength of the *prima facie* case presented and the necessity for the disclosure of the anonymous defendant's identity to allow the plaintiff to properly proceed. These guidelines should be flexible, non-technical, and fact-sensitive and applied so as to prevent plaintiffs from using the discovery process to ascertain the identities of unknown defendants in order to harass, intimidate, or silence critics in the public forum opportunities presented by the Internet.

9. The appellate court concluded that plaintiff failed to satisfy two of the elements of a *prima facie* case for intentional infliction of emotional distress, even though the poster was angry with the plaintiff.

10. Accordingly, the appellate court ordered the trial court to quash the subpoena.

In re Anonymous Online Speakers, 611 F.3d 653 (9th Cir. 2010)

1. Quixtar sued TEAM, claiming TEAM orchestrated an Internet smear campaign via anonymous postings and videos.
2. During discovery Quixtar sought testimony from a TEAM employee regarding the identity of five anonymous online speakers who allegedly made defamatory statements about Quixtar.
3. The district court ordered TEAM to disclose the identity of three of the five speakers.
4. Both sides sought intervention from the appellate court, one side seeking to prevent disclosure of the information and the other side seeking to compel.
5. The Ninth Circuit noted that anonymous public speech in America stretches back at least to *The Federalist Papers* and papers published by their opponents, the Anti-Federalists.
6. The court said the ability to speak anonymously on the Internet promotes the robust exchange of ideas and allows individuals to express themselves more freely without fear of economic or official retaliation or concern about social ostracism.
7. The court determined that the speech at issue related solely to the economic interests of the speaker and, therefore, was properly categorized as commercial speech.
8. Commercial speech enjoys a limited measure of First Amendment protection, commensurate with its subordinate position on the scale of First Amendment values.
9. The court opined that the standard for allowing disclosure of the identity of anonymous commercial speakers should be lower than that for anonymous political speakers.
10. Here, the Ninth Circuit affirmed the district court’s decision to allow disclosure of the identities because the district court had concluded that disclosure was proper even under the most stringent standard for protecting the identities of anonymous speakers. That standard, adopted from *Doe I v. Cahill*, 884 A.2d 451 (Del. 2005), requires, among other things, that the speaker be notified of the request for his/her identity and that the requester be able to survive a hypothetical summary judgment motion on its claim for relief. The Ninth Circuit noted that there was a protective order in place which would protect sensitive matters that implicate First Amendment rights.

Salehoo Group, Ltd. v. ABC Co., 2010 WL 2773801 (W.D. Wash. 2010)

1. Court said the weight of authority favored applying a test modeled after *Dendrite, Int'l, Inc. v. Doe No. 3,* 775 A.2d 756 (N.J. Super. Ct., App. Div. 2001).

2. Court applied a four-part test. First, the plaintiff must undertake reasonable efforts to give the defendant adequate notice of the attempt to discover his or her identity and provide a reasonable opportunity to respond. Second, the plaintiff must, in general, allege a facially valid cause of action and produce *prima facie* evidence to support all the elements of the cause of action within his or her control. Thus, the strength of the plaintiff's case must be evaluated before he or she is permitted to unmask by subpoena an anonymous defendant. There must be sufficient evidence to create a jury issue on the underlying claim.

   The court recognized that, at an early stage of the litigation, a plaintiff may not possess information about the role played by every defendant or other evidence that could be obtained through discovery. Third, the plaintiff must demonstrate that the specific information sought by subpoena is necessary to identify the defendant and that the defendant's identity is relevant to the plaintiff's case. Fourth, where the preceding factors do not present a clear outcome, the court should balance the interests of the parties. In doing so, the court should assess and compare the magnitude of harms that would be caused to the competing interests by a ruling in favor of the plaintiff and a ruling in favor of the defendant.

The Mortgage Specialists, Inc. v. Implode-Explode Heavy Indus., Inc., 999 A.2d 184 (N.H. Sup. Ct. 2010) (adopting the *Dendrite* test)

McVicker v. King, 266 F.R.D. 92 (W.D. Pa. 2010)

1. Plaintiff sued, claiming he was terminated in violation of various federal and state anti-discrimination laws.

2. Plaintiff filed a motion to compel disclosure of identities of seven persons who posted anonymous statements on a website near the time the borough council dismissed plaintiff.

3. The owner of the website, Trib Total Media, informed plaintiff that it objected to the subpoena and would not produce any names without a court order.

4. The court said a party seeking disclosure must clear a higher hurdle where the anonymous poster is a non-party to the lawsuit.

5. The trend among courts is to hold that entities such as newspapers, ISPs, and website hosts may, under the principle of *jus tertii* standing, assert the rights of their readers and subscribers.

6. Trib Total Media's privacy policy emphasized TTM's intention to protect the privacy of its users and expressly stated that TTM may "disclose your information in response to a court order, at other times when the Company believes it is reasonably required to do so . . . ."

7. That privacy policy created an expectation of privacy for any registered user.

8. Court denied the motion to compel the identities because the court was not persuaded that the plaintiff needed the identities in order to impeach the individual defendants.

In re Rule 45 Subpoena Issued to Cablevision Systems Corp. Regarding IP Address 69.120.35.31, 2010 WL 2219343 (E.D.N.Y. 2010)

1. An anonymous person posted on Internet message boards numerous messages that were critical of Prospect and its employees.

2. Prospect issued a subpoena to Yahoo! seeking user information on several posters.

3. The magistrate judge for the federal district court stated that, in addition to a First Amendment right to engage in anonymous speech, the poster has a privacy interest in maintaining the confidentiality of his/her identity and whereabouts as a customer of Cablevision, the ISP.

4. The magistrate judge said many federal courts have applied the test enunciated in *Sony Music Entm't Inc. v. Does 1-40,* 323 F. Supp. 2d 556 (S.D.N.Y. 2004).

5. The magistrate judge utilized the following five factors in analyzing the poster's First Amendment right to anonymous speech and the plaintiff's desire to obtain the poster's identity: (a) the nature of the speech of the anonymous Internet user; (b) the nature and strength of the claims and defenses of the party seeking the discovery; (c) the importance of the identifying information to such claims and defenses; (d) the availability of other sources of information; and (e) the conduct and relationship of the parties and subpoenaed party.

6. The magistrate judge found these facts to be significant: A number of factors in addition to the identity of the poster would play a role in whether Prospect prevailed in the lawsuit; Prospect could present its arguments without knowing the poster's identity; as a publicly traded company, Prospect is necessarily the subject of rumors and speculation; and, most

importantly, there is no evidence the trustee relied upon the postings in making any significant decisions.

7. Accordingly, the magistrate judge recommended granting Doe's motion to quash the subpoena.

Sedersten v. Taylor, 2009 WL 4802567 (W.D. Mo. 2009) (court determined this was not the exceptional case that warranted disclosure of the identity of an anonymous, non-party speaker who posted critical comments on a newspaper's Internet site)

Cohen v. Google, Inc., 887 N.Y.S. 2d 424 (Supreme Ct., N.Y. Cty. 2009) (court held that plaintiff was entitled to pre-action disclosure of identity of anonymous blogger who made allegedly defamatory statements about the plaintiff, including use of the words skank, skanky, ho, and whoring)

Solers, Inc. v. Doe, 977 A.2d 941 (D.C. Ct. App. 2009)

1. Plaintiff software developer filed suit against John Doe and served a subpoena on SIIA (which describes itself as the principal trade association for the software and digital content industry), seeking the identity of Doe, who purportedly defamed plaintiff.
2. SIIA enables sources with knowledge of software piracy to report them anonymously by Internet or telephone.
3. Doe reported by Internet that plaintiff had engaged in illegal activity.
4. An interesting aspect of this case is that Doe did not post his accusations on an internet bulletin board. Instead, he apparently followed the instructions on SIIA's website and used the internet to report his allegations directly and more privately.
5. The appellate court set out a five-part test for the District of Columbia to use in addressing these requests for the identity of anonymous Internet sources.
6. The appellate court remanded to give the parties the opportunity to present evidence in accordance with the newly-adopted test.

Doe I v. Ciolli, 611 F. Supp. 2d 216 (D. Conn. 2009)

1. Holding that the presence of pseudonymous defendants does not destroy diversity jurisdiction.
2. Defendant's postings on the Internet site specifically targeted plaintiffs in Connecticut, providing long-arm, personal jurisdiction.

3. Defendant had sufficient contacts to satisfy due process because he purposely and repeatedly posted messages about the plaintiffs. He knew that: (a) the plaintiffs were law students; and (b) he had posted the messages on a message board which was viewable by the plaintiffs and their classmates.

Enterline v. Pocono Med. Ctr., 2008 WL 5192386 (M.D. Pa. 2008) (Plaintiff filed a sexual harassment suit against her employer; she served a subpoena on a non-party newspaper, seeking the identities of persons who posted anonymous comments on the newspaper's Internet site and who claimed to possess information related to plaintiff's sexual harassment suit; plaintiff failed to establish that the information was not available from other sources; therefore, the court denied plaintiff's motion to compel)

Doe I v. Individuals, 561 F. Supp. 2d 249 (D. Conn. 2008)

1. Does I and II, both female law students, filed suit against 39 unknown individuals who the plaintiffs alleged made defamatory, threatening, and harassing statements on an Internet site. Among the postings were statements about the women's breasts, the posters' desire to have sexual relations with the women, the alleged criminal history of Doe II's father, and gay lovers.
2. Plaintiffs issued a subpoena to AT&T for information regarding the identities of the posters.
3. The federal district court concluded that plaintiffs' interest in pursuing discovery outweighed defendant Doe 21's First Amendment right to speak anonymously.
4. Consequently, the court denied Doe 21's motion to quash the subpoena.

Krinsky v. Doe 6, 72 Cal. Rptr. 3d 231 (Cal. Ct. App. 2008)

1. The court noted that many Internet sites allow users (a/k/a posters) to express themselves anonymously by using screen names traceable only through the hosts of the sites or their Internet service providers (ISPs). The use of pseudonymous name offers a safe outlet for the user to experiment with novel ideas, express unorthodox political ideas, or criticize corporate or individual behavior with fear of intimidation or reprisal.
2. The court also noted that the poster's message may be passed onto to an expanding number of recipients as readers may copy, forward, or print those messages.
3. Yahoo! warned its users that it will reveal their identifying information when legally compelled to do so.

Greenbaum v. Google, Inc., 845 N.Y.S.2d 695 (Supreme Ct., N.Y. Cty. 2007) (Courts recognize a difference between a statement of opinion that implies a basis in facts that are not disclosed and a statement of opinion that is accompanied by a recitation of facts on which it is based. The latter ordinarily are not actionable because a proffered hypotheses that is offered after a full recitation of the facts on which it is based is readily understood by the audience as conjecture.)

McMann v. Doe, 460 F. Supp. 2d 259 (D. Mass. 2006) (addressing First Amendment, defamation, and jurisdiction issues)

Best Western Int'l, Inc. v. Doe, 2006 WL 2091695 (D. Ariz. 2006) (adopting a "summary judgment standard" for analyzing requests for identities of anonymous posters)

Doe I v. Cahill, 884 A.2d 451 (Del. Sup. Ct. 2005)

1. Plaintiff-appellant Cahill was a city council member.
2. Defendant-appellee Doe I posted two statements on an Internet website sponsored by a news organization. The statements criticized Cahill including stating that he has "character flaws, not to mention an obvious mental deterioration. Cahill is a prime example of failed leadership . . . ."
3. Cahill filed a defamation suit against four Doe defendants.
4. During discovery Cahill sought to have the ISP, Comcast, provide the identity of Doe I.
5. If the ISP knows the date and time that a posting was made from a specific IP address, the ISP can determine the identity of its subscriber.
6. According to the court, the Internet is a unique democratizing medium unlike anything that has come before. The advent of the Internet dramatically changed the nature of public discourse by allowing more and diverse people to engage in public debate. Speakers can reach an enormous audience.
7. Because Internet speakers can remain anonymous, the audience must evaluate a speaker's ideas based upon her words.
8. Anonymous Internet speech in blogs or chat rooms can become the modern equivalent of political pamphleteering.
9. In general our society accords greater weight to the value of free speech than to the dangers of its misuse.
10. The First Amendment does not protect defamatory speech.

11. The revelation of identity of an anonymous speaker may subject the speaker to ostracism for expressing unpopular ideas, invite retaliation from those who oppose her ideas or from those whom she criticizes, or simply give unwarranted exposure to her mental processes.

12. Court held that, before a defamation plaintiff can obtain the identity of an anonymous defendant through compulsory discovery process, the plaintiff must satisfy the following obligations. First, to the extent reasonably practical under the circumstances, the plaintiff must undertake efforts to notify the anonymous poster that he is the subject of a subpoena or application for order of disclosure. The plaintiff must also withhold action to afford the anonymous defendant a reasonable opportunity to file and serve opposition to the discovery request. When a case arises in the Internet context, the plaintiff must post a message notifying the anonymous defendant of the plaintiff's discovery request on the same message board where the allegedly defamatory statement was originally posted. Second, the plaintiff must support his defamation claim with facts sufficient to defeat a summary judgment motion. Thus, the plaintiff must submit sufficient evidence to establish a *prima facie* case for each essential element of the claim in question.

13. Finally, the court held that Cahill had failed to establish a prima *facie case* of defamation because a reasonable person would have realized the statements about Cahill were only opinion and not facts.

Sony Music Entertainment Inc. v. Does 1 – 40, 326 F. Supp. 2d 556 (S.D.N.Y. 2004) (anonymity is a shield from the tyranny of the majority)

Polito v. AOL Time Warner, Inc., 2004 WL 3768897 (Pa. Ct. Common Pleas 2004) (Internet users who choose to violate the law by transmitting harassing or defamatory communications should not be entitled to conceal their identity and avoid punishment or liability for their actionable conduct)

Immunomedics, Inc. v. Doe, 775 A.2d 773 (N.J. Superior Ct. 2001)

1. Plaintiff Immunomedics filed suit against anonymous poster on Internet site that a suspected employee had posted information that was confidential and proprietary to the corporation. Plaintiff alleged the posted information violated the company's confidentiality agreement and several provisions of the company's employee handbook.

2. Plaintiff served on Yahoo! a subpoena seeking discovery of the poster's identity.

3. Plaintiff corporation presented sufficient evidence that the poster was a current or former Immonumedics employee and that all employees are bound by several company policies and a confidentiality agreement.
4. The court stated that there must be an avenue for redress of those who are wronged. Individuals choosing to harm another or to violate an agreement through speech on the Internet cannot hope to shield their identity so as to avoid punishment through invocation of the First Amendment.
5. The court concluded that disclosure of the poster's identity was warranted.

First Amendment, Miscellaneous Issues:

U.S. Supreme Court:

Reno v. ACLU, 117 S. Ct. 2329 (1997)

1. U.S. Supreme Court upheld the district court's entry of preliminary injunction against enforcement of the provisions of the Communications Decency Act.
2. The Court found the CDA was too vague, particularly considering that it utilized content-based regulation of speech and was a criminal statute.
3. The Court also found the CDA to be overly broad.
4. Significantly, the Court recognized that "[t]hrough the use chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox."

Courts other than the U.S. Supreme Court:

People v. Hickman, 988 P.2d 628 (Colo. 1999) (discussing interplay of First Amendment and threats)

Privacy:

Fourth Amendment to the U.S. Constitution provides in pertinent part:

> "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated ..."

U.S. Supreme Court:

City of Ontario v. Quon, 130 S. Ct. 2619 (2010)

1. City of Ontario, CA had a Computer Usage, Internet and E-Mail Policy that applied to all employees. The policy provided that the city:

> "reserves the right to monitor and log all network activity including e-mail and Internet use, with or without notice. Users should have no expectation of privacy or confidentiality when using these resources."

2. Quon was a member of the Ontario Police Department.
3. The city issued Quon a pager, which was subject to the computer policy set forth above.
4. Quon signed a statement acknowledging that he had read and understood the computer policy.
5. The computer policy did not expressly reference text messages.
6. However, the city informed its employees that it would treat text messages the same as it would treat e-mails.
7. The city limited its employees with pagers to a certain number of characters per billing cycle.
8. Because Quon and another employee regularly exceeded the character limit, the city reviewed transcripts of their text messages to determine whether the character limits were too low or whether those two employees were sending personal messages.
9. The city learned that many of the messages Quon sent were personal messages, some of which were sexually explicit.
10. The city disciplined Quon, who sued under 42 U.S.C. § 1983 and the Stored Communications Act (18 U.S.C. § 2701, et seq.).
11. The Fourth Amendment guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the government without regard to whether the government actor is investigating crime or performing another function.
12. The court found that the search of Quon's text messages was justified at its inception because there were reasonable grounds for suspecting that the search was necessary for a noninvestigatory, work-related purpose: To determine whether the city's character limit on text messages was sufficient to meet the city's needs. The scope of the search justified because reviewing the transcripts was an efficient and expedient way to determine whether Quon's overages were the result of work-related or personal messages.
13. Even if Quon had some level of privacy in his text messages, due to the city's informing its employees of the computer policy, it was not reasonable for him to think his messages would always be secure from city scrutiny.

14. It is not necessary that the search be conducted in the least intrusive manner because that could raise insuperable barriers to the exercise of all search and seizure powers. For all these reasons, the search was reasonable.

15. The Court noted that it must proceed with care when considering the whole concept of privacy expectations made on electronic equipment owned by a government employer. There are rapid changes in both the dynamics of communication and information transmission and in what society accepts as proper behavior.

O'Connor v. Orteg*a*, 107 S. Ct. 1492 (1987)

1. Searches and seizures by government employers or supervisors of the private property of their employees are subject to the restraints of the Fourth Amendment.

2. In evaluating what privacy expectations society is prepared to accept as reasonable, the Supreme Court has given weight to such factors as the intention of the Framers of the Fourth Amendment, the uses to which the individual has put a location, and our societal understanding that certain areas deserve the most scrupulous protection from government invasion.

3. Public employees' expectations of privacy in their offices, desks, and file cabinets may be reduced by virtue of actual office practices and procedures or legitimate regulation.

4. The employee's expectation of privacy must be assessed in the context of the employment relation – it is the nature of government office that fellow employees, supervisors, consensual visitors, the general public, and others may have frequent access to an employee's office.

5. The standard of reasonableness applicable to a particular class of searches requires balancing the nature and quality of the intrusion on the employee's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion.

6. Thus, courts must balance the employee's legitimate expectations of privacy against the government's need for supervision, control, and the efficient operation of the workplace.

7. Public employees are entrusted with tremendous responsibility; and the consequences of their misconduct or incompetence to both the agency and the public can be severe.

8. Because government offices are provided to employees for the sole purpose of facilitating the work of an agency, employer intrusions into employees' workplace involve a relatively limited invasion of employee privacy.

9. The Court held that public employer intrusions on the constitutionally protected privacy interests of government employees for both noninvestigatory, work-related purposes and investigations of work-related misconduct should be judged by the standard of reasonableness.

10. A search must be: (a) justified at its inception; and (b) as actually conducted, reasonably related in scope to the circumstances which justified the interference in the first place. Ordinarily, a search of an employee's office by a supervisor will be justified at its inception when there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct or that the search is necessary for a noninvestigatory work-related purpose such as to retrieve a file. The search will be permissible in its scope when the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of the nature of the misconduct.

Courts other than the U.S. Supreme Court:

Jennings v. Jennings, 697 S.E.2d 671 (S.C. Ct. App. 2010)

1. E-mails stored on Yahoo's server were in "electronic storage" and were stored "for purposes of backup protection" for purpose of the Stored Communication Act.

2. SCA's prohibition against intentionally accessing without authorization an electronic communication service facility does not extend to persons who did not access the facility but instead were provided information by a person who did access it.

Crispin v. Christian Audigier, Inc., 2010 WL 2293238 (C.D. Cal. 2010) (addressing the SCA and social networking websites)

Moreno v. Hanford Sentinel, Inc., 91 Cal. Rptr. 3d 858 (Cal. Ct. App. 2009) (court said information disclosed to a few people may remain private; however, there was no reasonable expectation of privacy in posting on popular social network website of disparaging comments about author's hometown because comments could be distributed to a vast audience)

Brown-Criscuolo v. Wolfe, 601 F. Supp. 2d 441 (D. Conn. 2009)

1. In determining whether an employee has a reasonable expectation of privacy in e-mails sent or received on his/her employer's computer or e-mail system, the court should consider four factors.

2. First, does the employer maintain a policy banning personal or other objectionable use;
3. Second, does the employer monitor the use of the employee's computer or e-mail;
4. Third, do third parties have a right of access to the computer or e-mails; and
5. Fourth, did the employer notify the employee of, or was the employee aware of, those employer policies relating to computer usage?

Discovery – Attorney-Client Privilege Issues:

Green v. Beer, 2010 WL 3422723 (S.D.N.Y. 2010) (plaintiffs did not waive attorney-client privilege with respect to e-mails that plaintiffs' counsel sent to technically unskilled plaintiffs through their son)

Stengart v. Loving Care Agency, Inc., 990 A.2d 650 (N.J. Sup. Ct. 2010) (courts have found that the existence of a clear company policy banning personal e-mail messages can diminish an employee's claim to privacy of e-mail messages between the employee and his/her attorney; here, plaintiff had a reasonable expectation of privacy in e-mails with her attorney because she used a personal, password-protected e-mail account and did not save the e-mails on the employer's computer)

Forward v. Foschi, 27 Misc. 3d 1224(A) (N.Y. Supreme Ct., Westchester Cty. 2010) (discussing waiver of attorney-client privilege)

Ranch v. Cty. of Boise, 2009 WL 3669741 (D. Idaho 2009) (plaintiff waived attorney-client privilege as to e-mails where governmental employer put its employees on notice that e-mails: (a) would become property of the employer; (b) would be monitored, stored, accessed, and disclosed by the employer; and (c) should not be considered confidential)

Ledbetter v. Wal-Mart Stores, Inc., 2009 WL 1067018 (D. Colo. 2009) (protective order covers information sought from social network sites)

U.S. v. Etkin, 2008 WL 482281 (S.D.N.Y. 2008) (employees do not have a reasonable expectation of privacy in the contents of their work computers when their employers communicate to them a policy under which the employer may monitor or inspect the computers at any time)

Scott v. Beth Israel Med. Ctr. Inc., 847 N.Y.S.2d 436 (Supreme Ct., N.Y. Cty. 2007) (employer's policy of no personal e-mails and allowing monitoring of the system vitiated plaintiff's attorney-client privilege in the e-mails)

Long v. Marubeni Am. Corp., 2006 WL 2998671 (S.D.N.Y. 2006) (plaintiffs' disregard of employer's e-mail policy stripped the confidential cloak from the e-mails)

Curto v. Med. World Communications, Inc., 2006 WL 1318387 (E.D.N.Y. 2006) (plaintiff did not waive privileges attached to e-mails where her laptops were not connected to the employer's servers and were not located in the employer's office, thus preventing the employer from monitoring or intercepting plaintiff's e-mails; also, before returning the laptop to her employer, plaintiff deleted all her personal files, making it reasonable for her to believe that her personal documents remained confidential)

In re Asia Global Crossing, Ltd., 322 B.R. 247 (S.D.N.Y. 2005) (discusses right to privacy as to computer files and e-mails)

People v. Jiang, 33 Cal. Rptr. 3d 184 (Cal. Ct. App. 2005) (criminal defendant's belief that his attorney-client communications were confidential was objectively reasonable; no reason to believe that employer would make any effort to gain access to information in documents on employee-issued computer where documents were segregated as personal and password-protected)

Other Discovery Issues:

Barnes v. CUS Nashville, LLC, 2010 WL 2265668 (M.D. Tenn. 2010) (Magistrate judge offered to create a Facebook account if two witnesses were willing to accept the magistrate judge as a "friend" on Facebook solely for the purpose of reviewing photographs and related comments *in camera*. After reviewing and disseminating to the parties any relevant information, the magistrate judge would close the Facebook account.)

EEOC v. Simply Storage Mgmt., LLC, 2010 WL 3446105 (S.D. Ind. 2010)

1. EEOC filed suit against defendant business for alleged sexual harassment of two complainant women by a supervisor.

2. Defendant sought discovery of electronic copies of the profiles and all other information and statements on the Facebook and MySpace accounts of the two sexual harassment complainants. The basis for seeking the information was that the complainants had allegedly placed their emotional health at issue beyond that typically encountered with garden variety emotional distress claims. The EEOC objected to production as overly broad, not

relevant, unduly burdensome, and harassing and embarrassing to the complainants.

3. The court stated that discovery of social network sites ("SNS") requires the application of basic discovery principles in a novel context.

4. The court said the challenge was to define appropriately broad limits on the discoverability of social communications in light of a subject as amorphous as emotional and mental health and to do so in a way that provides meaningful direction to the parties.

5. A person's expectation and intent that her communications be maintained as private are not legitimate bases for shielding those communications from discovery.

6. Merely locking a profile from public access does not prevent discovery, either.

7. When privacy or confidentiality concerns have been raised, those interests can be addressed by an appropriate protective order.

8. SNS content must be produced when it is relevant to a claim or defense in the case. The substance of the communication – rather than the fact of communication – determines relevance. Although anything a person says or does might, in some way theoretical sense, be reflective of her emotional state, that possibility does not justify requiring the production of every thought the person may have reduced to writing or of depositing everyone with whom she may have talked. Nevertheless, it is reasonable to expect severe emotional or mental injury to manifest itself in some SNS content. Examination of that content might reveal information relating to the onset of such injuries and the degree of distress.

9. The court decided that some degree of SNS discovery was warranted in the subject case. The court determined that the appropriate scope of relevance is any profiles, postings, or messages and SNS applications for the two claimants during the relevant time period that reveal, refer, or relate to any emotion, feeling, or mental state or any communications that reveal, refer, relate to events that could reasonably be expected to produce a significant emotion, feeling, or mental state.

10. Pictures of the claimants during the relevant period would generally be discoverable because the context of the picture and the claimant's appearance may reveal the claimant's emotional or mental state. In general a picture or video of someone else is unlikely to be discoverable.

11. Facebook is not used as a means by which account holders carry on monologues with themselves.

12. A protective order to limit disclosure of certain discovery materials might be useful as to SNS content.

Major Tours, Inc. v. Colorel, 2009 WL 3446761 (D.N.J. 2009) (discovery of e-mail on back-up tapes)

Bass v. Miss Porter's School, 2009 WL 3724968 (D. Conn. 2009) (Defendants sought text messages and information on plaintiff's former Facebook account that were allegedly related to plaintiff's teasing and taunting. Plaintiff provided some documents to defendants. The court reviewed *in camera* documents not produced, found some to be relevant, and ordered them produced.)

Arteria Property PTY Ltd. v. Universal Funding V.T.O., Inc., 2008 WL 4513696 (D.N.J. 2008) (spoliation of website evidence)

Ex parte Cooper Tire & Rubber Co., 987 So.2d 1090 (Ala. Sup. Ct. 2007) (discovery of e-mails)

Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004) (improper disclosure of e-mails by Internet service provider (ISP) pursuant to defendant's invalid and overly broad subpoena)

Civil Litigation, Miscellaneous:

Mackelprang v. Fidelity Nat'l Title Agency of Nevada, 2007 WL 119149 (D. Nev. 2007)

1. Plaintiff sued her employer for sexual harassment, alleging that two Fidelity vice-presidents sent her inappropriate and sexually explicit e-mails and coerced her into having sexual relations under the threat that, if she did not, her husband (who also worked for Fidelity) would be fired.
2. Defendant Fidelity served a subpoena on MySpace.com to obtain two MySpace.com Internet accounts allegedly set up by plaintiff.
3. Fidelity contended that one of those MySpace account allegedly indicated that plaintiff did not want kids while the other MySpace account allegedly identified plaintiff as a 39-year old married woman with six children and stated that she loved all her children.
4. MySpace produced certain "public" information regarding the two accounts but refused to produce private e-mail messages on either account in the absence of a search warrant or letter of consent for production by the owner of the account. Plaintiff refused to consent to production of the private

messages on the grounds that the information was not relevant and improperly invaded plaintiff's privacy.

5. The court noted that in a sexual harassment case a plaintiff's workplace-related sexual behavior, including sexually provocative speech or dress, can be admissible to support a defense that defendant's conduct was not unwelcome or that defendant had reasonable grounds to believe it was not unwelcome.

6. However, Fed. R. Evid. 412(a), which limits the admissibility of evidence offered to prove the sexual behavior or sexual predisposition of any alleged victim, aims to safeguard the alleged victim against the invasion of privacy, potential embarrassment, and sexual stereotyping that is associated with public disclosure of intimate sexual details and the infusion of sexual innuendo into the fact finding process. The rule also encourages victims of sexual misconduct to institute and participate in legal proceedings against alleged perpetrators.

7. The court stated that courts have often allowed discovery of work related sexual behavior but not non-work related sexual behavior because a person may view conduct that is acceptable in his/her private life as off-limits at work.

8. The court determined that defendant Fidelity was engaging in a fishing expedition because its interest in the accounts was based only on suspicion and speculation.

9. The court concluded that Fidelity had not demonstrated a relevant basis for production of plaintiff's MySpace.com private e-mail messages.

Evidence:

U.S. v. Drummond, 2010 WL 1329059 (M.D. Pa. 2010) (motion in limine to exclude as evidence in a criminal trial photographs of defendant on his MySpace page)

Victaulic Co. v. Tieman, 499 F.3d 227 (3d Cir. 2007) (courts should be wary of taking judicially notice of facts on websites)

Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534 (D. MD. 2007) (lengthy discussion of evidentiary issues relating to electronically stored information ("ESI") including preliminary rulings on admissibility (Fed. R. Evid. 104); relevance (Fed. R. Evid. 401, 402, and 105); authenticity (Fed. R. Evid. 901 and 902) of e-mail, Internet website postings, text messages and chat room content, computer stored records and data, computer animation and computer simulations, and digital photographs; hearsay (Fed. R. Evid. 801-807); the original writing rule

(Fed. R. Evid. 1001-1008); and balancing probative value against the danger of unfair prejudice (Fed. R. Evid. 403).

Telewizja Polska USA, Inc. v. Echostar Satellite Corp., 2004 WL 2367740 (N.D. Ill. 2004) (admission of exhibit to show what a website looked like on a particular date; authentication of a redacted e-mail)

In re Homestore.Com, Inc. Securities Lit., 347 F. Supp. 2d 769 (C.D. Cal. 2004) (authentication of e-mails)

Discipline cases:

State v. Mandi, 2009 WL 2869943 (N.J. Superior Ct., App. Div. 2009) (court upheld dismissal of defendant police officer who was convicted of a petty disorderly conduct violation for creating a false and offensive profile of a female co-employee on MySpace.com.)

Cromer v. Lexington-Fayette Urban Cty. Gov't, 2008 WL 4000180 (E.D. Ky. 2008) (plaintiff police officer was dismissed due to allegedly inappropriate postings on a social networking site regarding an arrest plaintiff had made)

Pietrylo v. Hillstone Restaurant Group, 2008 WL 6085437 (D.N.J. 2008) (employee created an invitation-only group on MySpace.com for employees of defendant Hillstone to vent about the employer; the posts included sexual remarks about management and customers, jokes about customer service and quality, references to violence and illegal drug use, and a copy of a new wine test to be given to employees; after members of management were afforded access to the site, they fired two members of the group; there was a question of fact as to whether a member of the group had voluntarily consented to allowing management to view the site)

Garrity v. John Hancock Mutual Life Ins. Co., 2002 WL 974676 (D. Mass. 2002) (plaintiffs who voluntarily communicated sexually explicit jokes over the employer's e-mail system had no privacy interests in those communications; furthermore, defendant employer had a legitimate business interest in dismissing plaintiffs for sending the offensive e-mails because federal and state laws require employers to take affirmative steps to maintain a workplace free of sexual harassment and to investigate and take prompt and effective remedial action when potentially harassing conduct is discovered)

ADC Telecommunications ERISA Lit., 2005WL2250782 (D. Minn. 2005) (plaintiff was fired for posting an internal memo on a message board)

Statutes:

18 U.S.C. § 2701, et seq.
47 U.S.C. § 551 et seq.

Other Sources:

1. Blogging and Social Media in the Workplace and Beyond, SR0005 ALI-ABA 493 (2010)
2. Redefining Privacy in the Era of Social Networking, 53-SEP Advocate (Idaho) 27 (2010)
3. How Private is Facebook, 10/4/2010 N.Y.L.J. § 2, col.2, § 2 (2010)
4. Invasion of Privacy by Internet or Website Postings, 54 ALR6th 99 (2010)
5. Right of Privacy, 14 ALR2d 750 (1950)
6. Data Security and Privacy Law: Combatting Cyberthreats §9.79, Employer Policies (2010)
7. Internet and Online Law § 8.02, Privacy Considerations (2010)
8. Privacy, Free Speech and Blurry-Edged Social Networks, 50 B.C.L.Rev. 1315, (2009)
9. Hiring and Firing in the Facebook Age, 56 No. 5 Proc. Law 19 (2010)
10. Investigating Employee Conduct §§ 6:2, 6:42 (Blogs and Social Media), 11:08 (Right to Remain Anonymous) (2010)
11. Legal Issues Arising out of Employees' Use of Social Networking Sites, 10/5/2009 N.Y.L.J. 3, col.2 (2009)
12. Off-duty Privacy: How Far can Employers Go?, 37 N.Ky.L.Rev. 287 (2010)
13. On the Precipice of E-Discovery: Can Litigants Obtain Employee Social Networking Web Site Information through Employers?, 18 Comm. Law Conspectus 487 (2010)
14. Internet Law in the Courts, 13 No. 1 J. Internet L. 27 (2009)
15. Civil Discovery of Social Networking Information, 39 S.W.L.Rev. 413 (2010)
16. "Tweet" This: The Ethics of Social Networking, 79-May J. Kan.B.A. 17 (2010)
17. 191 New Jersey L.J., Drafting the Electronic Communication Policy (2008)
18. Social Media and the Workplace: Another Look, 5/13/2010 N.Y.L.J. 5, col.1 (2010)

19. Employment Issues Arising in Internal Investigations, 8/11/2008 N.Y.L.J. 11, col.1 (2008)

20. Blogging while (Publicly) Employed: Some First Amendment Implications, 47 U. Louisville L. Rev. 679 (2009)

21. Sex Based Employment Discrimination § 26 (2010)

22. Social Networking Sites: The Next E-Discovery Frontier, 66-NOV Bench and Bar Minn. 22 (2008)

23. Does What Happens on Facebook Stay on Facebook?, Discovery, Admissibility, Ethics and Social Media . . ., 98 Ill.B.J. 366 (2010)

24. Social Networking Sites and Personal Injury Litigation, 9/22/2009 N.Y.L.J. 3, col.1 (2009)

25. The Advent of Digital Diaries . . ., 9/22/2009 N.Y.L.J. 3, col.1 (2009)

26. Facebook isn't Your Space Anymore . . ., 58 U.Kan.L.R. 1279 (2010)

27. Twitigation . . ., 49 Washburn L. J. 841 (2010)

28. Whose Space?, 6 Internet Law and Strategy 1 (2008)

29. The Proof is in the Posting – How Social Media is Changing the Law, 73 Tex. B. J. 188 (2010)

30. First Amendment Protection Afforded to Website Operators, 30 ALR6th 299 (2008)

31. Right of Corporations, Absent Specific Subpoena Power, to Disclosure of Identities, 120 ALR5th 195 (2204)

32. Say What? Blogging and Employment in Conflict, 27 Columbia L. J. and Arts 145 (2003)

33. 2006 Duke L. and Tech. Rev. 2, Anti-Employer Blogging (2006)

34. Bloggers Beware: Blogging and At-Will Employment, 24 Hofstra Lab. & Empl. L. J. 333 (2007)

35. Reasonable Measures to Protect Trade Secrets in a Digital Environment, 49 Idea 359 (2009)

36. Legal Risks of Electronic Surveillance in the Workplace, 35 Fed. Md B. J. 3 (2008)

37. 191 N.J. L.J. 885, What are Employers to do about Social Media and Potential Liability from Blog Postings? (2008)

38. Hiding from the Boss . . ., 23 Santa Clara Computer & High Tech L. J. 135 (2006)

39. Brave New Cyberworld: Employer’s Legal Guide to Internet, 24 Lab. Law 109 (2008)

40. First Amendment Protection for Blogs and Bloggers, 35 ALR6th 407 (2008)

41. Prockauer on Privacy § 9.3.8, Blogging and Cybersmearing (2010)

42. Balancing Act: Finding Consensus for Unmasking Internet Speakers, 51 B.C. Law Rev. 833 (2010)

43. Anonymity in Cyberspace: What can we Learn from John Doe?, 50 B.C. Law Rev.1373 (2009)

44. Cyber Civil Rights, 89 B.U.L.R. 61 (2009)

45. 67 Am. Jur. Proof of Facts 3d 249, Proof of Liability for Violation of Privacy of Internet User, by Cookies or Other Means (2010)

46. 100 Am. Jur. Proof of Facts 3d 89, Proof of Instant Message, Blog or Chat Room as Evidence (2010)

APPENDIX VI

Social Networking, Counterintelligence, and Cyber Counterintelligence

Rebecca J. Rohan

CYB 615 Z1 - Cyber Counterintelligence

APA Citation Style

June 18, 2011

http://www.onlineuticacollege.com/programs/masters-cybersecurity.asp

rjrohan@utica.edu

Executive Summary

This paper discusses intelligence, counterintelligence, cyber counterintelligence, and use of social networking. In order to relate counterintelligence (CI) and cyber counterintelligence (CCI) to social networking, CI and CCI are explained. CI involves an organization recognizing that it is the target of intelligence operations and takes measures to deny or negatively influence intelligence collection. CCI is CI executed via cyber means. The intelligence life cycle is discussed as process of planning and direction, collection, processing, analysis and production, and dissemination to intelligence consumers. CI and CCI fit into the intelligence life cycle as an organization executes measures to impact, influence, or impede the intelligence life cycle of an adversary collecting intelligence against it.

Social networking is discussed along with applications of social networking by criminals, the United States, foreign governments, law enforcement, and employers. Once applications of social networking are presented, relationships will be drawn between social networking applications and CI methods including deception and counterintelligence operations. Legal, ethical, and privacy issues surrounding the use of social networking will be presented.

With the understanding of social networking applications, CI methods, and various issues, protective measures for both individuals and organizations will be discussed. Discussion of how social networking issues and the intelligence life cycle will be presented. Suggestions for how individuals, organizations, and intelligence analysts can identify and remediate issues in using social networking will be noted. Understanding the importance of social networking and its related issues will better prepare individuals, organizations, and intelligence agencies to employ it wisely.

Contents

Introduction

The focus of this paper is social networking and relating its use to intelligence, counterintelligence, and cyber counterintelligence. An explanation of the terms counterintelligence (CI) and cyber counterintelligence (CCI) will be presented. The intelligence life cycle will be discussed and how CI fits into the cycle. Social networking will be defined prior to discussing applications of social networking in intelligence and CCI. Discussion of relating social networking and CCI to intelligence and CI methods will also be presented. Legal, ethical, and privacy issues concerning social networking and CCI will be discussed. Methods to protect a person or organization from CCI when using social networking are presented. Lastly, analysis of social networking and CCI to the intelligence life cycle along with problem identification and remediation will be discussed.

Counterintelligence, and Cyber Counterintelligence

Before discussing social networking and its applications in conducting cyber counterintelligence, the terms intelligence, counterintelligence (CI), and cyber counterintelligence (CCI) must be explained. As defined by Vincent Bridgeman, CI is "the broad subset of intelligence focused on the intelligence efforts of a competitor" with the aim to understand and exploit that competitor's reliance on intelligence (Ehrman, 2009). Per Executive Order 12333, CI is "information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities" (What, n.d.). Simply, CI is an organization's identification of intelligence collection against it by a competitor and the actions taken by the organization taken to impede or prevent that intelligence collection.

Understanding what CI is, cyber counterintelligence or CCI can be explained. The Department of Defense (DoD) defines CCI as the "measures to identify, penetrate, or neutralize foreign operations that use cyber means as the primary tradecraft methodology, as well as foreign intelligence service collection efforts that use traditional methods to gauge cyber capabilities and intentions" (Cyber, n.d.). CCI is counterintelligence that "deals specifically with the added capabilities and vulnerabilities of computers and computer networks" (French & Kim, 2009, p. 72). With CI and CCI defined, the intelligence life cycle can be presented and how CI relates to the cycle.

The Intelligence Life Cycle and Counterintelligence

To better understand CI and CCI, the intelligence life cycle is presented. Intelligence is more than the product of collection and analysis. Intelligence is a process or life cycle comprised of five steps:

1. Planning and Direction,
2. Collection,
3. Processing,
4. Analysis and Production, and
5. Dissemination (The Commission, 2005, p. 584).

The intelligence life cycle begins with intelligence consumers—policymakers, military officials, and other decision makers—identifying their requirements (The Commission, 2005, p. 583). The identified requirements drive the planning and direction of collection activities with collected information then being analyzed and processed into reports for dissemination back to the intelligence consumers (The Commission, 2005, p. 583-584). During dissemination, intelligence consumers provide feedback that may indicate further requirements to collect and analyze additional information in order to fully meet the consumers' needs (The Commission, 2005, p. 584). As illustrated in Figure 1, the intelligence life cycle is a continuous process with no definitive beginning or ending point.

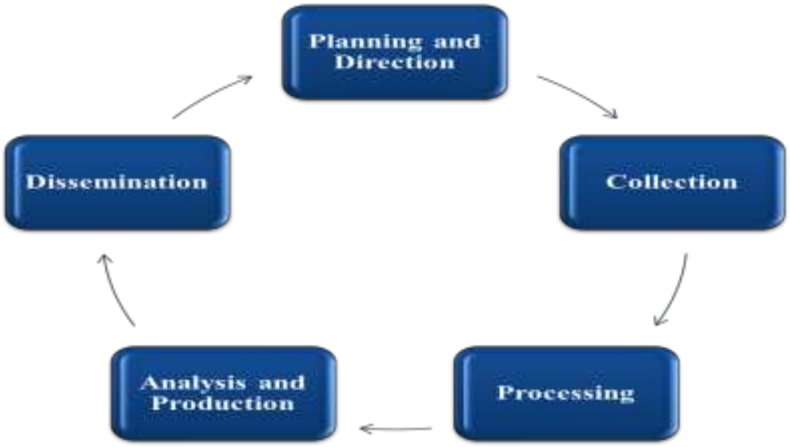


Figure 1 – The Intelligence Life Cycle. Source: Adapted from Testing the Intelligence Cycle Through Systems Modeling and Simulation by Judith M. Johnston and Rob Johnston, available at www.cia.gov.

With knowledge about the intelligence life cycle, relationships can be made between CI and CCI and the intelligence life cycle. As opposed to collecting intelligence for consumers, CI has been simply defined as intelligence activities taken by a competitor and actions to stop those intelligence activities with CCI incorporating the use of cyber as a CI capability or vulnerability. "Counterintelligence involves at its core an ongoing intelligence cycle focused narrowly on the competitor's intelligence efforts and decision making, plus additional activities conducted to degrade the competitor's intelligence capability or manipulate the competitor's decisions to achieve a policy outcome" (Sims & Gerber, 2009, p. 128). From a different point of view, CI and CCI fit into the intelligence life cycle as requirements identified after detecting intelligence collection against an organization by a competitor. Identification of the competitor's intelligence collection then leads to planning and directing of actions to stop or inhibit the competitor's collection. The goal is to impede the competitor's processing, analyzing, synthesizing, and disseminating of intelligence to his consumers about the target organization. Ultimately, CI and CCI follow the steps of the intelligence life cycle with the goal to damage or halt the competitor's intelligence collection against its target. Understanding CI, CCI, and the intelligence life cycle, social networking will be discussed.

What is (Cyber) Social Networking?

In order to discuss the applications of social networking for cyber counterintelligence (CCI), the concept of social networking must be explained. Social networking is more than just Facebook or Twitter. Social networking is composed of all web-based services allowing users to do three things:

1. Build a public or semi-public user profile within a bounded system.
2. View a list of other users sharing something in common or a connection.
3. "View and traverse their list of connections and those made by others within the system (Boyd & Ellison, 2007).

Social networking software encompasses all applications that "connect people and information in spontaneous, interactive ways" and can be grouped into categories including:

- "personal social networks (Facebook),
- blogs (WordPress),
- microblog (Twitter),
- audio (BlogTalkRadio),
- video (YouTube),
- collaborative tools (GoogleDocs), and
- wikis (TWiki)" (Drapeau & Linton, 2009, p. 2).

Social networking allows users to interact with friends, reestablish connections with lost acquaintances, and create connections to new friends. While interacting with friends and acquaintances, users will share personal information without hesitation. The House Subcommittee on Crime, Terrorism, and Homeland Security noted in a hearing that "the dramatic increase in the popularity of social networking sites has perhaps overshadowed some of the risk of sharing too much information in those forums" while "social networking sites provide the opportunity and the temptation to incrementally put more and more personal information into cyberspace" (Subcommittee, 2010, p. 3). With valuable information being freely posted to social networking sites, individuals and organizations can use cyber methods to gather intelligence or conduct cyber counterintelligence for use in a variety of applications.

Applications of Social Networking in Intelligence and CCI

With users posting valuable information on social networking sites, individuals and organizations can gather and use that information in a variety of applications. In this section, applications of social networking for both intelligence and CCI purposes will be presented. Discussion will include the application of social networking in intelligence and CCI by:

- individuals or organizations to commit crimes,
- the United States (U.S.) internally on its own citizens,
- the United States externally against other countries or organizations,
- foreign governments against other countries,
- law enforcement against individuals or groups, and

- employers on prospective/current employees.

Application by Individuals/Organizations to Commit Crimes

Social networking sites can be used by individuals or organizations to commit crimes. In using social networking sites, criminals may conduct intelligence operations to collect information or facilitate commission of crimes. To facilitate commission of crimes, social networking sites have been used as command and control channels for malware networks. A discovery in August 2009 uncovered the use of Twitter as a command and control channel for malware designed to steal banking credentials from compromised computers in Brazil (Shadows, 2010, p. 21). In another situation, a private Google Group was being used as a command control channel to issue commands to compromised computers, which responded back to the private Google Group (Shadows, 2010, p. 21).

Besides facilitating commission of crimes, social networking sites can provide criminals with valuable personal information. Criminals gathering user data from various social networking sites may obtain enough personal information to answer the security questions for resetting that user's password to online accounts (Subcommittee, 2010, p. 2). Burglars have used social networking sites to determine the best time to break into users' homes based on the users' posts about being at work or away on vacation (Subcommittee, 2010, p. 2). After hijacking users' Facebook accounts, criminals will send distress calls to friends of the hijacked users requesting money to be wired to accounts controlled by the criminals (Subcommittee, 2010, p. 2). In addition to increased use of social networking sites by scammers and spammers, hackers use social networking sites to spread malware such as viruses and Trojan horses (Federal Agents, 2010).

If enough personal information is collected by criminals, social networking users may be vulnerable to identity theft. Per Mr. Pasqua of Symantec, posting information such as birthdates and mother's maiden names provides valuable information for criminals to use to commit identity theft, crack passwords, takeover accounts, send spam, or distribute malware (Subcommittee, 2010, p. 54). Mr. Snow also noted that social networking sites can be used for the purposes of social engineering, fraud, phishing, data mining, and as a communication tool for the cyber underground (Subcommittee, 2010, p. 8-11).

Criminals and criminal organizations may use social networking sites to avoid law enforcement and communicate with each other. Mexican drug cartels are using Twitter to "circumvent dragnets and communicate with one another" (Okeowo, 2010). To avoid detection, the cartels use key words that mean one thing to them but something else to people outside the cartels (Okeowo, 2010). These key words can be part of a YouTube video of a song with "lyrics that contain subtle clues as to the current hierarchies of gangs—as well as threats" (Okeowo, 2010). Cartels have also used social networking sites to spread fear and disrupt people's lives in towns such as Reynosa with threats of convoys of hitmen visiting the town (Okeowo, 2010). Social networking sites have provided cyber capabilities for criminals in conducting crimes and avoiding detection.

Application by the United States Internally

The United States has turned to social networking sites in conducting operations within its borders. The Department of Homeland Security (DHS) conducted CCI operations to monitor social networking sites during the inauguration of President Obama during January 2009 (Federal Agents, 2010). Prior to and during Obama's inauguration, DHS's Social Networking/ Media Capability (SNMC) reviewed social networking sites for noteworthy items per established Critical Information Requirements or CIRs (Social, 2009, p. 8). The SNMC also implemented trend analysis to detect reportable events. To be considered for trend analysis, items had to be:

- from credible, verifiable sources;
- backed by credible evidence such as videos or photos;
- corroborated from multiple sources indicative of a trend; and
- noted in official alerts at any level including local, state, or national (Social, 2009, p. 9).

Since June 22, 2010, the SNMC has been authorized to create user profiles for monitoring of social networking sites (Privacy, 2010, p. 3). However, these SNMC user profiles cannot:

- "actively seek personally identifiable information (PII);
- post any information;
- actively seek to connect with other internal/external personal users;
- accept other internal/external personal users' invitations to connect; or

- interact on social media sites" (Privacy, 2010, p. 3).

In certain situations, the DHS SNMC can collect PII on specific categories of individuals if the PII "lends credibility to the report or facilitates coordination with federal, state, local, tribal, territorial, foreign, or international government partners" (Privacy, 2010, p. 5). The specific categories of individuals include:

- "U.S. and foreign individuals *in extremis* situations involving potential life or death circumstances;
- Senior U.S. and foreign government officials who make public statements or provide public updates;
- U.S. and foreign government spokespersons who make public statements or provide public updates;
- U.S. and foreign private sector officials and spokespersons who make public statements or provide public updates; and
- Names of anchors, newscasters, or on-scene reporters who are known or identified as reporters in their post or article or who use traditional and/or social media in real time to keep their audience situationally aware and informed.
- Current or former public officials who are victims of incidents or activities related to Homeland Security
- Known terrorists, drug cartel leaders, or other persons known to have been involved in major crimes or terror of Homeland Security interest who are killed or found dead" (Privacy, 2010, p. 5).

In addition to the DHS SNMC using social networking sites to monitor U.S. citizens and internal events, other U.S. Government organizations have used social networking sites in conducting investigations or surveillance. The U.S. Citizenship and Immigration Services have used social networking sites to gather information and conduct surveillance for use in investigation of citizenship petitions (Lynch, 2010). The U.S. Government also had a Terrorist Surveillance Program to covertly monitor social networking tools, telephones, and email (Carafano, 2011). The U.S. has used social networking sites in monitoring events and conducting operations against foreign governments. Even the Internal Revenue Service (IRS) has searched social networking sites to help in “locating taxpayers and determining their online business activity” (Chesler, 2011).

Application by the United States Externally

The U.S. has used social networking sites in conducting surveillance and monitoring of world events and on foreign governments. The Department of State and U.S. Embassies have used social networking sites to monitor public opinion, potential threats, and developing trends within foreign countries (Mayfield, 2011, p. 80). This information helps the U.S. in developing policy or even in determining when to extract U.S. officials out of foreign countries due to dangerous political climates. The U.S. military is working with a software developer on an “online persona management service” allowing military users to create and control fake online personas, called sock puppets, to “influence internet conversations and spread pro-American propaganda” in Middle Eastern countries (Fielding & Cobain, 2011). The software contract requires the capabilities for 50 U.S.-based handlers to control the sock puppets in activities such as blogging on foreign-language websites in the efforts to “counter violent extremist and enemy propaganda outside the U.S.” (Fielding & Cobain, 2011).

One U.S. internal application of social networking sites is also being used for external applications. The Department of Homeland Security’s (DHS’s) Social Networking/Media Capability (SNMC) monitored information on social networking sites to provide situational awareness and establish a common operating picture during rescue and recovery efforts after Haiti’s earthquake in January 2010 (Privacy Compliance, 2010, p. 2). DHS’s SNMC also monitored social networking sites during the 2010 Winter Olympics in Vancouver for information related to border control, security, and safety (Privacy Compliance, 2010, p. 2). SNMC analysts would scan social networking sites for predefined search terms to find items of interest which would be noted for trend analysis (Privacy Compliance, 2010, p. 3). SNMC analysts would also monitor social networking sites for activity “hot spots” that would be further researched to identify issues for concern (Privacy Compliance, 2010, p. 4). Information about world events assists the U.S. Government in developing plans of action and identifying areas requiring additional research.

Application by Foreign Governments

Foreign governments use social networking sites for monitoring events internally and in gathering information about the U.S. With the increased use of social networking sites by U.S. military and government personnel, foreign countries can easily obtain valuable information about U.S. Operations. In speaking to the U.S. House Subcommittee on Crime Terrorism, and Homeland Security, Mr. Gordon Snow, the Assistant Director of the Federal Bureau of Investigation's (FBI's) Cyber Division, noted that inadvertent release of valuable information by government or military personnel on social networking sites can provide foreign governments with creditable intelligence (Subcommittee, 2010, p. 8). Foreign governments and even terrorist organizations search social networking sites for pieces of information when combined together can provide valuable intelligence about America's activities. Not only do foreign governments use social networking sites to monitor the U.S., foreign governments use social networking sites to monitor internal events.

Egypt and other foreign governments are monitoring social networking sites to gauge the political climate in an attempt to detect political uprisings in advance (Apps, 2011). If the Egyptian government had monitored social networking sites in 2008, the Egyptian government would not have been surprised by political unrest leading up to a protest held on April 6, 2008 (Drapeau & Linton, 2009, p. 20). Two Egyptian citizens started a prodemocracy Facebook group in late March 2008 to protest government policies including the policy of not allowing groups of more than five people to gather without first obtaining a permit (Drapeau & Linton, 2009, p. 20). Within a week of the groups' creation, the Facebook group grew to 40,000 members (Drapeau & Linton, 2009, p. 20). When the protest was held on April 6, 2008, Egyptian security forces were surprised by and unprepared for the number of protestors (Drapeau & Linton, 2009, p. 20). With monitoring, the Egyptian government could have been prepared for the protest and may have been able to avoid the protests by changing the policies questioned by citizens.

If Great Britain's government and law enforcement would monitor social networking sites, incidents involving the British royalty and the chief of MI6 could have been avoided. Recently, Prince Charles and Camilla were trapped in their car during a riot in London. If police had monitored Twitter messages coordinating protests, law enforcement could have rerouted the convoy carrying Prince Charles and Camilla to avoid the riot (Apps, 2011). In another incident, the British government could have avoided the release of personal information of the new MI6 chief. In July 2009, Sir John Sawers, the new MI6 chief, had personal information exposed when his wife posted personal information and photographs about their family on her Facebook page (Lewis, 2009). With no privacy protection on the Facebook account, any user could obtain information about the Sawers family including where the family lived and worked, who their friends were, and where they traveled on vacation (Lewis, 2009). Had the British government been monitoring social networking sites both incidents could have been averted.

Other countries have used social networking sites to deal with internal affairs. Iran has turned to social networking sites as tools of propaganda and deception. During the Iranian election protests, the Iranian government used Twitter and other social networking sites to spread misinformation (Carafano, 2009, p. 4). India has recognized social networking as a tool for information for both its people and its criminals. After terrorist attacks in Mumbai, India in November 2008, it was rumored that the Indian government was trying to stop the Twitter stream to prevent the terrorists using the Twitter information to avoid capture (Beaumont, 2008).

Israel has recognized the impact of social networking sites on military operations. When an Israeli soldier posted details of an upcoming raid on his Facebook page, Israeli Defense Forces stopped execution of the raid (Israeli, 2010). The information posted by the Israeli soldier included the raid's location, planned start time, and name of the unit conducting the raid (Israeli, 2010). Fortunately, the soldier's friends on Facebook alerted the Israeli military in time to stop the raid (Israeli, 2010). If the target of the raid had obtained this information, Israeli soldiers could have been seriously hurt or even killed. Information in the wrong hands can be deadly.

Application by Law Enforcement

Law enforcement (LE) uses social networking applications for various aspects of its operations including undercover operations, tracking and identifying criminals, and predicting crimes. During undercover operations, law enforcement agents can communicate with unsuspecting targets, access additional information, and discover social relationships (Lynch & Ellickson, n.d., p. 32). Evidence obtained from social networking sites can "reveal personal communications, establish motives and personal relationships, provide location information, prove and disprove alibis, and establish crime or criminal enterprise" (Lynch & Ellickson, n.d., p. 11). LE has used Facebook and Twitter to bust gang members from posted photographs showing identifiable tattoos, inscribed gang necklaces, stolen money, and stolen guns or from videos on YouTube showing cars that have been used in committing crimes (Lipowicz, 2011).

Social networking sites can also provide LE with evidence or even information to stop crimes. Evidence discovered when investigating social networking sites can be used by LE as leverage during interrogations. If a suspect denies attending a party, a photograph from the suspect's Facebook page may prove otherwise (Chesler, 2011). LE may also use social networking sites to predict or even stop crimes. Using customer relationship management software, LE agencies can monitor chatter on social networking sites for predictive analysis and identify the potential for an outbreak of violence before it ever occurs (Chesler, 2011).

Besides police, lawyers are using social networking sites to support their cases. Prosecuting attorneys use social networking sites to research information about witnesses and diagram social networks (Lynch & Ellickson, n.d., p. 33). On the contrary, defense attorneys for criminal suspects may search Facebook and other social networking sites for profiles of law enforcement officers looking for incriminating evidence that could be used against the officers in court (Lipowicz, 2011).

Application by Employers

Employers are using social networking sites to obtain information about prospective employees and current employees. Employers and corporate recruiters will use social networking sites to view profiles of prospective employees to determine if the individuals would fit in with the company's culture or to uncover any potentially damaging information about the prospective employees (Moore, 2011). The California Public Agency Labor and Employment Blog noted, "A prospective employer may legally use social media if the information obtained is publicly available (i.e. not password protected) and is posted by the job applicant (e.g. Facebook)" (Morin & Arce, 2011). Employers have also used information from social networking sites during litigation and when conducting investigations (Moore, 2011).

Employers have punished and even fired employees based on information posted on social networking sites even if the information is posted outside duty hours. Employees can be disciplined for posting information that

- "undermines its [a company's] mission, purpose, and credibility with the public";
- includes "harassment, bullying or other conduct that affects the agency";
- "violates agency rules or policies"; or
- "discloses proprietary information" (Morin & Arce, 2011).

After using his Facebook page to criticize the Philadelphia Eagles for failing to keep safety Brian Dawkins on the team, an employee of the team was fired in March 2009 (Moore, 2011). Furthermore, an employee's off-duty conduct on social networking sites can also be subject to discipline.

Relating Social Networking and CCI to CI Methods

The stated applications of social networking can be related to counterintelligence methods. In order to discuss these relationships, counterintelligence methods must be discussed and defined. Counterintelligence operations or counteroperations can be grouped into four categories:

1. Passive defense including security systems, locks, or classification rules aimed at keeping valuable information away from opponents.
2. Active defense including surveillance, interrogations, and wiretapping aimed at determining the offensive actions of opponents.
3. Passive offense including camouflage, fake weapons, or hiding assets within "innocuous-looking buildings" aimed at distorting opponents' perceptions and influencing opponents' decisions.
4. Active offense including "duping the adversary by directly feeding false information to him and manipulating his interpretation of it" (Sims & Gerber, 2009, p. 21-23).

In reviewing these four categories, a common theme of altering perceptions and deceptions becomes evident. While perception is how an individual views the world, deception is changing an individual's perception to a false view of the world (Sims & Gerber, 2009, p. 70-71). Deception can be employed to destroy other's perceptions and intelligence as well to turn an organization's counterintelligence efforts against it (Sims & Geber, 2009, p. 75). The key for deception to be successful is in understanding how the target perceives. "People's perceptions are strongly driven by their needs and expectations, which are difficult for senders to comprehend, let alone manipulate (Sims & Geber, 2009, p. 78). Keeping in mind the four categories of counteroperations and the concepts of perception and deception, the previously stated applications of social networking can be related to CI methods.

Referring to the four categories of counteroperations listed above, examples of each category can be identified from the applications of social networking noted in this paper.

1. Passive defense is illustrated by the classification of information as sensitive or classified and policies stipulating users should not post sensitive or classified information on social networking sites.
2. Active defense is illustrated in the actions of the DHS's SNMC in conducting surveillance to determine threats against the President during the inauguration or border threats during the 2010 Winter Olympics.
3. Passive offense is illustrated when hackers fool users into following links that download and install malware under the guise of viewing something innocent.
4. Active offense is illustrated in scenarios where the U.S. military use fake personas or sock puppets to spread propaganda and disinformation.

Instances of employing deception are common throughout applications of social networking. Deception schemes via social networking sites can result in military or government workers inadvertently divulging national security information. In one scheme, an individual posed as an attractive female intelligence analyst with profiles on various social networking sites and then sent friend requests to members of the military, government, and defense contractors (Subcommittee, 2010, p. 7). The individual was able to gather a reasonable amount of sensitive data to include a picture from a soldier on patrol in Afghanistan that contained embedded data about the soldier's location (Subcommittee, 2010, p. 7). People will allow unknown, unvetted people access to view their social networking profiles without confirming identities. In one situation, "a private Internet security company was able to view highly personal information from 40 percent of 200 Facebook users who chose to add a fictitious member to their Facebook accounts. The company created this fictional member to illustrate now vulnerable people can be when using social networks." (Subcommittee, 2010, p. 16).

Other deception applications via social networking sites are not limited to revealing information or accessing user profiles. Attackers use social engineering techniques to trick social networking users into “downloading malware or divulging sensitive information under the auspice that they are doing something perfectly innocent” (Subcommittee, 2010, p. 59). Social networking sites can be used to conduct “information operations (the integrated employment of electronic warfare, computer network operations, psychological operations, deception, and operations security)” (Carafano, 2011). During the election protests, the Iranian government used social networking sites to publish propaganda and disseminate disinformation (Carafano, 2011).

For an unknown deceptive purpose, Tom MacMaster, an American student studying in Scotland, admitted that he was the author of the blog “A Gay Girl in Damascus” (Ambrogi, 2011). This blog chronicled the life of a lesbian activist, Amina Abdallah Arraf al-Omari, in Syria during the recent period of civil unrest (Ambrogi, 2011). Recent posts on the blog stated that Amina was abducted which prompted online campaigns demanding Amina’s release (New post, 2011). MacMaster claims his intent was “to get information out” and that “the facts behind the narrative were true” (Ambrogi, 2011). Campaigners for gay and political rights claim the fictitious blog has “harmed their cause and potentially endangered lives” (Ambrogi, 2011).

During the Iranian election protests, social networking users attempted to stop the spread of disinformation by the Iranian government. “Twitspam, a social-networking site that encourages users to identify and block malicious ‘tweeters’ on Twitter, hosted an interactive Web page where users discussed possible ‘Iranian agents’ operating online” (Carafano, 2009, p. 4). Social networking sites were used as a medium to organize attacks on the Iranian government’s websites and databases (Carafano, 2009, p. 7). These acts of “Hacktivism” aimed at disrupting or taking the Iranian government offline via denial-of-service attacks and distributing disruptive software for others to use (Carafano, 2009, p. 7). Clearly, social networking applications are vehicles for executing CI methods.

Legal, Ethical, and Privacy Issues

Using social networking sites for intelligence and CI purposes is not exempt from a plethora of issues—legal, ethical, and privacy. In terms of legal issues, one issue could be the

U.S. military's use of the "online persona management service" on U.S. citizens. If the "online persona management service" being developed for the U.S. military was used against U.S. citizens, it could be legally challenged for engaging in sock puppetry—using fake online personas (Fielding & Cobain, 2011). However, if the software is used against foreign individuals, it does not present the legal issue. In another legal issue in September 2010, a real estate lawyer was convicted of identity theft and criminal impersonation for establishing email accounts and pretending to be a professor admitting to plagiarizing information about the Dead Sea Scrolls (Eligon, 2010). The lawyer claimed that the target of his campaign—the professor-actually plagiarized from his father, but the court viewed his actions as being a legal issue (Eligon, 2010).

Other issues in using social networking sites could be labeled as legal and ethical issues. Because many members of the military use social networking sites to communicate with family and friends especially during deployments, operational security (OPSEC) can be compromised through posted information. One piece of information posted by one social networking user may be harmless. If several users post different pieces of information, connecting the dots between those pieces of information can be damaging to military operations (Weaver, 2009). Price Floyd, Principal Deputy Assistant Secretary of Defense for Public Affairs, noted that a letter with sensitive information might only be read by a few people while a post on Twitter or Facebook has the potential to be seen by thousands of people (Weaver, 2009). If the information posted is deemed as being sensitive or classified, the individual responsible could be punished legally. Ethically, it could be an issue especially for compromising the safety of military personnel and possibly their families. The impact of posting sensitive or classified information on social networking sites is much greater with the information potentially being accessible to thousands of people.

Using social networking sites can result in violations of privacy. When monitoring social networking sites for threat or violence trends, accidental collection of personally identifiable information (PII) can happen. When the DHS Privacy office conducted a privacy compliance review of the DHS's Social Networking/Media Capability (SNMC), it was noted that accidental collection of PII can happen (Privacy, 2010, p. 3). However, the SNMC must take steps to redact any PII collected to protect individual privacy (Privacy, 2010, p. 3). If the PII is related to exceptional circumstances involving life or death situations, then the PII will not be redacted (Privacy, 2010, p. 3).

In addition, only the "user-generated information posted to publicly available online forums, blogs, public websites, and message boards are retained" with no information about the individuals responsible for the posts (Privacy, 2010, p. 4). Privacy is also protected by ensuring that reports and information are only shared with individuals with the need to know (Privacy, 2010, p. 5). SNMC personnel are also trained in redaction of PII with charts about PII and redaction being posted at personnel workstations (Privacy, 2010, p. 6).

Use of social networking sites for employment pre-screening can result in privacy or legal issues. To avoid issues with screening prospective employees' profiles on social networking sites, employers can implement steps to protect against discrimination claims. Employers should have policies in place regarding the use of social networking sites when conducting background checks and ensure the policies are applied consistently in all background checks (Moore, 2011). Employers also need to be careful about encountering user-protected information such as sexual orientation or disabilities when viewing prospective employees' social networking profiles (Wallen & Flock, 2009). Employers need to be careful to base decisions on not hiring an individual on aspects that are not protected information. To further protect against discrimination suits, employers can employ impartial individuals or hire an outside agency separate from the hiring process to review social networking profiles to look for specific items to further minimize the risk of discrimination lawsuits. Being aware of the potential issues in using social networking sites, individuals and organizations can take actions to protect themselves.

Protective Measures When Using Social Networking

Understanding the issues surrounding the use of social networking sites, individuals and organizations can implement protective measures. The biggest and most important protective measure is user education. When working with House Subcommittee on Crime, Terrorism, and Homeland Security, the Symantec Corporation shared seven basic security measures for using social networking sites including:

1. Never share passwords to social networking sites.

2. Never post anything that should not be public knowledge.
3. Never post sensitive information such as a phone number, birthdate, or vacation status.
4. Ignore links with "enticing titles" sent by friends.
5. Verify posted links, such as on a Facebook wall, are valid links.
6. Limit those who can access a profile to family and friends.
7. Keep informed of changes to privacy policies of social networking sites (Subcommittee, 2010, p. 62).

Symantec also recommended the following "Social Networking Rules of Engagement" for children or young adults using social networking sites including:

- Do not post too much information that could identify you or your whereabouts.
- Use the site's privacy settings to restrict access to people you know and trust.
- Do not physically meet people you met online if you do not know them.
- Do not post suggestive images or pictures that could reveal your identity or location or affect others' perceptions of you.
- Review sites for compromising information posted by friends and delete anything you think is compromising or offensive.
- Do not lie about your age to gain access to specific sites.
- Do not provide any financial information without obtaining permission from your parents.
- Do not post about rumors or personal information that could implicate you or your parents. (Subcommittee, 2010, p. 62-63).

Governments can implement protective measures by understanding and implementing the four principles of counterdeception:

1. "Know yourself" by understanding one's vulnerabilities.
2. "Know your adversary" by understanding the adversary's culture, means and motive.
3. "Know your situation" by checking the environment for cues that deception is occurring.
4. "Know your channels" by verifying where information is derived (George & Bruce, 2008, p. 130-131).

In addition, governments should learn to counter denial and deception through active learning based on successes and failures of past performances; through practice in denial and deception scenarios; and pay attention to anomalies or incongruities (George & Bruce, 2008, p. 135).

Military personnel should also implement protective measures when using social networking sites. Military personnel using social networking sites should avoid using names, ranks, deployment dates, or equipment specifications/capabilities when posting information (U.S. Army, 2011). The U.S. Army Social Media Handbook listed "Security Items to Consider":

- "Take a close look at all privacy settings. Set security options to allow visibility to 'friends only'.
- Do not reveal sensitive information about yourself such as schedules and event locations.
- Ask, "What could the wrong person do with this information?" and "Could it compromise the safety of me, my family or my unit?"
- Geotagging is a feature that reveals your location to other people within your network. Consider turning off the GPS function of your smartphone.
- Closely review photos before they go online.
- Make sure they do not give away sensitive information, which could be dangerous if released.
- Make sure to talk to family about operations security and what can and cannot be posted.
- Videos can go viral quickly; make sure they don't give away sensitive information." (U.S. Army, 2011, p. 5).

The U.S. Army Social Media Handbook also recommends:

- not tagging photos with geographical locations;
- not using location-based social networking applications at locations that could compromise Army operations; and
- turning off the GPS function in smartphones when conducting Army operations (U.S. Army, 2011, p. 5).

The handbook notes that, "Failure to do so could result in damage to the mission and may even put families at risk." (U.S. Army, 2011, p. 5).

Organizations can implement protective measures for using social networking sites.

To reduce or eliminate the risk of sensitive or classified information being posted on social networking sites, an organization needs to stipulate in its policies what can and cannot be posted on both internal and external social networks site (Disruptive, 2010, p. 23). This policy must be provided to employees and should be displayed when an employee logs into a social networking site (Disruptive, 2010, p. 23). Social networking access policies should clearly define who can access external social networking sites and for what purposes and be enforced using automated controls (Disruptive, 2010, p. 23). To minimize the release of sensitive or classified information on external social networking sites, organizations should routinely search social networking sites for any damaging information and work with post's author or the site to have the information removed (Disruptive, 2010, p. 23). Implementing these various protective measures will help individuals and organizations from encountering issues when using social networking sites.

Issues of Social Networking, CCI, & the Intelligence Life Cycle

Individuals, organizations, and intelligence analysts need to be aware of the risks and pitfalls in using social networking sites. As noted in a previous section, perception can be easily manipulated for deception purposes when using or interacting with people on social networking sites. In particular, intelligence analysts need to be aware of the pitfalls with relying on social networking sites as sources of information. On the contrary, intelligence analysts can use social networking sites as a tool to protect information and thwart intelligence collection by adversaries. Intelligence analysts can employ passive denial by "better securing key information or other assets to prevent them from being obtained and exploited by a competitor" or active denial by "tying up the competitor's intelligence and decision-making effort with useless 'operational games'" (Sims & Gerber, 2009, p. 128). Feeding adversaries false information via social networking sites further promotes the denial of intelligence. "Denial is about preventing the competitor's intelligence service from conveying a decision advantage to the competitor's decision cycle" (Sims & Gerber, 2009, p. 128). Deception via social networking sites can manipulate adversaries into using their own intelligence channels "as a means to achieve an operational outcome through deception" (Sims & Gerber, 2009, p. 128). Conducting CI through social networking sites may provide intelligence analysts with an advantage by gaining insight to how competitor's intelligence cycle operates and use this insight in making decisions (Sims & Gerber, 2009, p. 128).

Looking back at the intelligence life cycle in Figure 1, deception and counteroperations can influence all steps of the intelligence life cycle. Based on the intelligence consumers' perceptions including perceptions based on deception, planning and direction could be misguided. Collection can be impacted by deception employed in posts on social networking sites and deceptive schemes executed by individuals or organizations on social networking sites. Skewing of collected information then impacts the steps processing, analysis and production, and dissemination. As long as individuals, organizations, and intelligence analysts are aware of the perils involved in using social networking sites, it will be harder for criminals and adversaries to influence perception and execute schemes of deception.

Conclusion

This paper addressed social networking and its applications in intelligence, counterintelligence (CI), and cyber counterintelligence (CCI). Knowledge of the terms CI and CCI along with knowledge of the intelligence life cycle helps to understand how intelligence and CI can be employed via social networking sites. Understanding the issues encountered during the different applications of social networking assist in preventing legal, ethical, and privacy issues as well as protecting individuals and organizations from potential issues associated with use of social networking. Discussion of perception, deception, and counterintelligence operations enables individuals, organizations, and intelligence analysts to be wary of social networking sites and to avoid falling prey to deception. Relating the intelligence life cycle to the issues of social networking further assists in avoiding the impacts of deception and executing deceptive schemes against other individuals and organizations.

References

Ambrogi, S. (2011, June 13). Activists slam Syria “Gay Girl” blog hoax. Reuters.com. Retrieved from http://www.reuters.com/article/2011/06/13/us-britain-syria-hoax-idUSTRE75C2AZ20110613.

Apps, P. (2011, February 8). Should spies spend more time on Twitter? Reuters. Retrieved from http://www.reuters.com/article/2011/02/08/us-technology-protest-spies-idUSTRE71726I20110208.

Beaumont, C. (2008, November 27). Mumbai attacks: Twitter and Flickr used to break news. The Telegraph. Retrieved from http://www.telegraph.co.uk/news/worldnews/asia/india/3530640/Mumbai-attacks-Twitter-and-Flickr-used-to-break-news-Bombay-India.html.

Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication, 13*(1), article 11. Retrieved from http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html.

Carafano, J. J. (2009, July 20). All a Twitter: How social networking shaped Iran’s election protests. Backgrounder, 2300. Retrieved from http://www.heritage.org/research/reports/2009/07/all-a-twitter-how-social-networking-shaped-irans-election-protests.

Carafano, J. J. (2011, January). Mastering the art of wiki: Understanding social networking and national security. *Joint Forces Quarterly 60*, 73-78. Retrieved from http://www.ndu.edu/press/social-networking-national-security.html.

Chesler, C. (2011, April 14). How cops are using social networks for crooks. Popular Mechanics. Retrieved from http://www.popularmechanics.com/technology/how-to/computer-security/how-cops-are-casing-social-networks-for-crooks.

Cyber counterintelligence. (n.d.). DoD Dictionary of Military Terms. Retrieved from http://www.dtic.mil/doctrine/dod_dictionary/.

Disruptive information technologies: Cloud computing, social networking, consumerization. (2010, September). Aerospace Industries Association. Retrieved from http://www.aia-aerospace.org/assets/report_ebiz_2010_web.pdf .

Drapeau, M., & Wills, L., III. (2009, April). Social software and national security: An initial net assessment. National Defense University-Center for Technology and National Security Policy. Retrieved from https://www.hsdl.org/?view&doc=109885&coll=limited.

Ehrman, J. (2009, August 24). Toward a theory of CI: What are we talking about when we talk about counterintelligence? *Studies in Intelligence, 53*(2). Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol53no2/toward-a-theory-of-ci.html.

Eligon, J. (2010, September 30). Son of Dead Sea Scrolls expert is convicted. The New York Times. Retrieved from http://www.nytimes.com/2010/10/01/nyregion/01scrolls.html.

Federal agents urged to 'friend' people on social networks, memo reveals. (2010, October 14). FoxNews.com. Retrieved from http://www.foxnews.com/scitech/2010/10/13/government-spying-social-networks/.

Fielding, N., & Cobain, I. (2011, March 17). Revealed: US spy operation that manipulates social media. The Guardian. Retrieved from http://www.guardian.co.uk/technology/2011/mar/17/us-spy-operation-social-networks.

French, G. S., & Kim, J. (2009). Acknowledging the revolution: The urgent need for cyber counterintelligence. National Intelligence Journal, 1(1), 71-90. Retrieved from http://lcwebs.net/2010/Acknowledging_%20the_Revolution.pdf.

George, R. Z., & Bruce, J. B. (2008). *Analyzing intelligence: Origins, obstacles, and innvoations*. Washington, D.C.: Georgetown University Press.

Israeli military 'unfriends' solider after Facebook leak. (2010, March 4). BBC News. Retrieved from http://news.bbc.co.uk/2/hi/8549099.stm.

Johnston, J. M., & Johnston, R. (2005). Testing the intelligence cycle through systems modeling and simulation. Center for the Study of Intelligence. Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/analytic-culture-in-the-u-s-intelligence-community/chapter_4_systems_model.htm.

Lewis, J. (2009, July 5). MI6 chief blows his cover as wife's Facebook account reveals family holidays, showbiz friends and links to David Irving. DailyMail Online. Retrieved from http://www.dailymail.co.uk/news/article-1197562/MI6-chief-blows-cover-wifes-Facebook-account-reveals-family-holidays-showbiz-friends-links-David-Irving.html.

Lipowicz, A. (2011, April 5). Agencies use social media to bust gangs. Federal Computer Week. Retrieved from http://fcw.com/articles/2011/04/05/law-enforcement-agencies-usiing-social-media-to-bust-gangs.aspx.

Lynch, J. (2010, October 13). New FOIA documents reveal DHS social media monitoring during Obama inauguration. Electronic Frontier Foundation. Retrieved from https://www.eff.org/deeplinks/2010/10/new-foia-documents-reveal-dhs-social-media.

Lynch, J., & Ellickson, J. (n.d.). Obtaining and using evidence from social networking sites. Department of Justice-Computer Crime & Intellectual Property Section. Retrieved from https://www.eff.org/files/filenode/social_network/20100303__crim_socialnetworking.pdf.

Mayfield, T. D., III. (2011, January). A commander's strategy for social media. *Joint Forces Quarterly, 60*, 79-83. Retrieved from https://www.hsdl.org/?view&doc=135910&coll=limited.

Moore, B. J. (2011, May 18). The evolution of social networking technologies in the workplace: Balancing employee and employer rights. The National Law Review. Retrieved from http://www.natlawreview.com/article/evolution-social-networking-technologies-workplace-balancing-employee-and-employer-rights.

Morin, P., & Arce, E. (2011, March 7). 10 things employers and employees should know about social media. California Public Agency Labor and Employment Blog. Retrieved from http://www.calpublicagencylaboremploymentblog.com/privacy/10-things-employers-and-employees-should-know-about-social-media/.

New post says Syrian 'Gay Girl' blogger is a hoax. (2011, June 13). CNN.com. Retrieved from http://edition.cnn.com/2011/WORLD/meast/06/12/syria.blogger/index.html.

Okeowo, A. (2010, April 14). To battle cartels, Mexico weighs Twitter crackdown. Time.com. Retrieved from http://www.time.com/time/world/article/0,8599,1981607,00.html.

Privacy compliance review of the 2010 Winter Olympics social media event monitoring initiative. (2010, August 23). U.S. Department of Homeland Security. Retrieved from http://www.dhs.gov/xlibrary/assets/privacy/privacy-privcomrev-ops-olympicsandhaiti.pdf.

Shadows in the cloud: investigating cyber espionage 2.0. (2010, April 6). Information Warfare Monitor & Shadowserver Foundation. Retrieved from http://www.f-secure.com/weblog/archives/Shadows_In_The_Cloud.pdf.

Sims, J. E., & Gerber, B. (2009). *Vaults, mirrors, & masks: Rediscovering U.S. counterintelligence*. Washington, D.C.: Georgetown University Press.

Social networking monitoring center (SNMC) concept of operations for the Presidential Inauguration. (2009, January). Department of Homeland Security. Retrieved from https://www.eff.org/files/filenode/social_network/DHS_SNMC_Inauguration_monitoring.pdf.

Subcommittee on Crime, Terrorism, and Homeland Security. (2010, July 28). Hearing on "Online privacy, social networking, and crime victimization." U.S. House of Representatives. Retrieved from http://judiciary.house.gov/hearings/hear_100728.html.

The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. (2005, March 31). Appendix C: An intelligence community primer. Retrieved from http://www.gpoaccess.gov/wmd/pdf/appendix_c_fm.pdf.

U.S. Army Office of the Chief of Public Affairs. (2011, January). U.S. Army social media handbook. Homeland Security Digital Library. Retrieved from https://www.hsdl.org/?view&doc=137789&coll=documents.

Wallen, V., & Flock B. (2009, May/June). Social networking sites pose risk for employers. The Online Journal for Certified Managers. Retrieved from http://cob.jmu.edu/icpm/management_world/prodmay09.pdf.

Weaver, H. F. (2009, September 23). Defense Department to announce balanced social media policy. Defense.gov. Retrieved from http://www.defense.gov/news/newsarticle.aspx?id=55948.

What is counterintelligence? (n.d.). Office of the National Counterintelligence Executive. Retrieved from http://www.ncix.gov/about.html.

APPENDIX VII

NEWS

Bill allows tougher penalties in social media based mob attacks

May 18, 2013 | By Naomi Nix | Tribune reporter

Recommend 2 Tweet 5 6

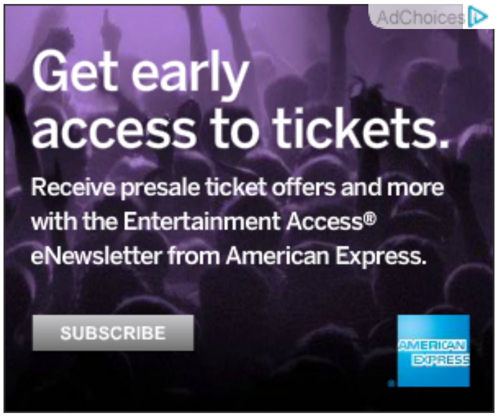
Gov. Pat Quinn signed into law Saturday legislation that calls for stiffer penalties on people who text or use social media to organize mob attacks.

Gov. Pat Quinn shakes hands with State Rep. Christian Mitchell o...

Social media has made it easier for groups of people to orchestrate violent crimes throughout the city, including those releated to gang activity and some recent problems along the Magnificent Mile shopping district in downtown Chicago, legislators said.

“As we know in recent months, we have had a serious problem with the use of social media to cause harm to people and property,” said Quinn, before signing the bill at Pioneer Court near Michigan Avenue and Wacker Drive. “We don’t want anyone using social media to harm anyone.”

State Sen. Kwame Raoul, D-Chicago, said police told him that there had been an incident recently where a young woman was shot by a rival gang member after she posted a picture on Facebook that revealed where she was at the time.



Related Links

RAW VIDEO: Organized violence bill press conference

Related Articles

Sherman Brought The Glare Of News Media On Himself
June 21, 1998

“That ought not be tolerated on Michigan Avenue and it ought not be tolerated on the South Side of Chicago,” said Raoul, who sponsored the bill.

Under the new law, which goes into effect immediately, judges have discretion to impose a more severe sentence on anyone who uses electronic media to organize a group of people to commit violent crimes.

Previously, those who were convicted of using electronic communication to organize violent mob action could face a prison sentence of between one and three years. The new law changes the potential prison time to between three and six years.

The new legislation only targets people who organize the criminal activities, though participants may be subjected to other penalties.

Critics of the bill have argued that it would drive up prison costs and have little effect on violence.

The measure sailed through the state senate and house. It was sent to the Governor on Friday, winning praise from business groups who say the attacks can deter tourists and local shoppers in downtown Chicago.

“We want to [retain] safe places for people to come and shop and enjoy our city,” said Illinois Retail Merchants Association vice president Tanya Triche, who attended Saturday’s signing.

nnix@tribune.com

Twitter: @nsnix87

New Deal In Media: One Am For An Fm
March 31, 1997

The Resurrection Of Old St. Pat`s
November 12, 1989

Burden of proof?
January 20, 2008

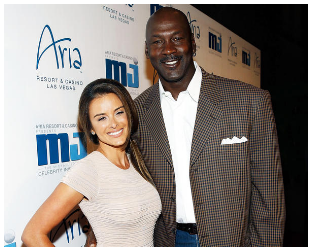
David Bar-Illan, 73, a concert pianist, former editor and...
November 9, 2003

Find More Stories About

Social Media
Michigan Avenue

Featured Articles

Decoding the diabetic diet



Michael Jordan marries longtime girlfriend

Age gap: She's old enough to be his ... wife

MORE:

Steps can be taken to relieve or prevent night leg cramps

Alarms should sound on deal

Can you solve the 'when to buy' conundrum?

An easier way to go

Try A Sample Mensa Test

17 puppies found abandoned near Indiana Dunes

APPENDIX VIII

FBI battling 'rash of sexting' among its employees

By Scott Zamost and Drew Griffin , CNN Special Investigations Unit

updated 5:35 AM EST, Fri February 22, 2013

CNN.com

Washington (CNN) -- It sounds like the plot of a bad movie: bugging your boss' office. Sending naked photos around to co-workers. Sexting in the office. Paying for sex in a massage parlor.

But it all happened in the federal agency whose motto is "fidelity, bravery, integrity" -- the FBI.

These lurid details are outlined in confidential internal disciplinary reports obtained by CNN that were issued to FBI employees as a way to deter misconduct.

Read the FBI's internal reports (PDF)

The FBI hopes these quarterly reports will stem what its assistant director called a "rash of sexting cases" involving employees who are using their government-issued devices to send lurid texts and nude photos.

"We're hoping (that) getting the message out in the quarterlies is going to teach people, as well as their supervisors ... you can't do this stuff," FBI assistant director Candice Will told CNN this week. "When you are given an FBI BlackBerry, it's for official use. It's not to text the woman in another office who you found attractive or to send a picture of yourself in a state of undress. That is not why we provide you an FBI BlackBerry."

While the vast majority of the FBI's 36,000 employees act professionally, the disciplinary reports issued by the agency's Office of Professional Responsibility show serious misconduct has continued for years.

From 2010 to 2012, the FBI disciplined 1,045 employees for a variety of violations, according to the agency. Eighty-five were fired.

The internal reports over the last year don't specify job titles, names or the location of the employees. Yet, they provide exact details of their misdeeds:

-- One employee engaged in a "romantic relationship with former boyfriend (now husband) knowing he was a drug/user dealer. Employee also lied under oath when questioned during the administrative inquiry about her husband's activities."

-- Another FBI worker "hid a recording device in supervisor's office. In addition, without authorization, employee made copies of supervisor's negative comments about employee that employee located by conducting an unauthorized search of the supervisor's office and briefcase." It said the employee "lied to investigators during (the) course of the administrative inquiry."

-- An FBI supervisor "repeatedly committed check fraud and lacked candor under oath."

-- One employee "was involved in a domestic dispute at mistress' apartment, requiring police intervention.

Employee was drunk and uncooperative with police" and "refused to relinquish his weapon, making it necessary for the officers to physically subdue him, take the loaded weapon and place employee in handcuffs."

-- In other cases, an employee was charged with DUI for the second time, one used a lost or stolen credit card to buy gas, and another was caught in a child pornography sting operation, according to the internal reports.

All of the employees in these cases were fired.

More FBI employees were disciplined for their transgressions, including one woman who -- according to the reports -- "used (a) personal cell phone to send nude photographs of herself to other employees" which "adversely affected the daily activities of several squads." Another FBI worker e-mailed a "nude photograph of herself to ex-boyfriend's wife." Both employees received 10-day suspensions.

Another who visited a massage parlor "and paid for a sexual favor from the masseuse" received a 14-day suspension. And an employee who used a government-issued BlackBerry "to send sexually explicit messages to another employee" was suspended for five days.

Will expressed surprise at some of the behavior outlined in the reports.

"As long I've been doing this ... there are days when I think 'OK, I've seen it all,' but I really haven't," Will said. "I still get files and I think, 'Wow, I never would have thought of that.'"

Some of the recent cases follow what CNN uncovered in 2011 after obtaining several years of the internal disciplinary reports. Those reports included incidents involving FBI employees sleeping with informants, a sex tape made by an agent and his girlfriend, tapping into FBI databases for unauthorized searches, viewing pornography on bureau computers and other cases of drunk driving.

The FBI Agents Association -- which advocates for active and former FBI agents -- said the incidents should be considered in the proper context.

"It is important to note that the ratio of disciplinary issues among FBI agents are among the lowest in the federal government and private sector," the association's president Konrad Motyka told CNN.

Watch The Situation Room with Wolf Blitzer weekdays at 4pm to 6pm ET and Saturdays at 6pm ET. For the latest from The Situation Room click here.

APPENDIX IX

70/13-6136

CITY OF HOUSTON

INTER OFFICE CORRESPONDENCE

TO: M. I. Montalvo, Executive Assistant Chief
Investigative Operations

FROM: Larry J. Yium, Deputy Director
Planning

VIA: Mark L. Curran, Assistant Chief
Staff Services Command

T. N. Oettmeier, Executive Assistant Chief
Support Operations

DATE: January 25, 2013

SUBJECT: **Police Agencies Use of Social Media**

The purpose of this correspondence is to give an introduction and literature review on police departments and their use of social media.

Definitions

- Social network – an online community of people with a common interest who use a website or other technologies to communicate with each other and share information, resources, etc. *Dictionary.com*
- Social media – forms of electronic communications (as websites for social networking and micro-blogging) through which users create online communities to share information, ideas, personal messages, and other content (as videos). *Webster Dictionary*

Overview

Social media encompasses many different technologies, yet the underlying goal is to encourage communication. Some examples of social media formats include: blogs, podcast, micro-blogging, video and social networking sites. In terms of a specific type of engagement, there are also many different social networking sites, some examples are: Facebook, Twitter, YouTube, LinkedIn, Pinterest.

Literature Review

Many different organizations are achieving dramatic benefits by using social media tools to reach out to the public, which is why law enforcement agencies, including HPD, have found immense use in these technologies. Departments are using these tools to share alerts and press releases as well as reach out to the community, to prevent and solve crimes. Though the "big three" of social media, Twitter, Facebook and YouTube, are heavily utilized by most police agencies, departments are finding their own unique ways to utilize the three as well as expand into utilizing other forms of social media.

The Arlington, Texas Police Department (APD) is home of the renowned "tweet-alongs". A tweet-along is essentially a virtual ride along that uses tweets, or messages sent via Twitter, to communicate with followers. Tweet-alongs typically are scheduled for a set number of hours, with an officer or designated tweeter, posting regular updates to Twitter about what they are seeing as patrol officers perform their normal on-duty routine. The tweet-alongs have been increasingly popular, and because of it APD's social media following has risen from 600 to 6000. APD now does tweet-alongs twice a month to sustain their community involvement. The Dallas and Milwaukee police departments have also started hosting tweet-alongs after seeing the work Arlington has been doing.

The Boston Police Department (BPD) has seen a rapid increase in crime-solving tips with the help of a text-a-tip program and a new Twitter campaign. The text-a-tip program allows residents to send anonymous text messages to the department's Crime Stoppers Unit. The texting tipsters receive an automatic reply: "Thx. We'll ask u a few questions." Then, special software blocks the tipsters' phone number as officers text back and forth with them. At the end, the software sends an automatic text message reminding the tipster to delete the conversation thread from their phone. Tips received by BPD run from homicides and drug deals to online suicide notes and bomb threats; people often text photos as documentation. BPD has also been engaging the public with a weekly Twitter hashtag - #MostWantedMonday, which links to photos of wanted suspects that are posted at the start of each week.

The Dallas Police Department (DPD), along with many other public safety agencies, is sending out text messages and email alerts about neighborhood crimes, traffic problems, and community events, just to name a few uses, to residents using www.nixle.com, a secured website designed for law enforcement. Unlike Twitter and Facebook, Nixle employs a thorough screening process to verify that every agency joining the Nixle service is authentic. Nixle gives citizens the flexibility to direct messages based on priority so that they can receive urgent information via text message and the rest via email.

DPD has also partnered with Nextdoor (www.nextdoor.com), a free, private, networking option for neighborhoods. Each Dallas neighborhood has its own local Nextdoor website, accessible only to residents of that neighborhood. Information shared on Nextdoor is only visible to members who live in the neighborhood and who have a verified address. DPD, however, is still able to post useful and important information to Nextdoor sites within the city.

The Philadelphia Police Department (PPD) launched a mobile version of their website, PhillyPolice.com that uses smartphone's GPS to share the nearest police precinct. A new smartphone app called iWatch Philadelphia, lets citizens submit tips with detailed location and suspect information. They can also attach images and video to help detectives solve crimes quickly. Those apps are available for download for Apple and Android devices.

PPD also uses Facebook, Twitter, and YouTube to engage the public to identify perpetrators unknown to police. As of December, 2012, PPD has made 112 arrests from the approximately 200 videos posted in this manner. They have recently added Pinterest to their platform. Pinterest has become the third most popular social medium, behind Facebook and Twitter.

The Seattle Police Department (SPD) launched a new initiative called "tweets-by-beat". With Tweets by Beat, citizens can follow or a view a Twitter feed of police dispatches in each of Seattle's 51 police beats. In order to protect crime victims, officers, and the integrity of investigations, calls are displayed one hour after a dispatcher sends the call to an officer, as to avoid onlookers. The feeds also do not include information about domestic violence calls, sexual assaults, and other certain types of crimes.

Houston Police Department

Currently, the department has several initiatives that incorporate one or more social media:

- *Facebook* The department currently has 32,750 fans and it grows by about 200 fans per week. This number reaches out to over eight (8) million targets on a monthly basis. Friends of friends, not necessarily fans of the page, have the option to see a positive reinforcement about HPD with a click of the button. The current reach and potential reach increases daily. In many cases, local media and in a few cases, national media have picked up the department's stories on Facebook and redelivered them via a news story telecast or additional social media blasts from within their individual companies.
- *Twitter* The department has over 3000 followers (growing daily) and with that, this tool has become an invaluable asset for HPD. It is used for notifications during emergency situations, crime fighting tips, catch a crook (tips) videos and pictures and also to dispense the Chief of Police message during media availability days that occur once a month.
- *Blog* Senior Officer Mike McCoy manages a blog @ http://www.hpdblog.com. With up to 5000 hits per day, the blog continues to grow and has become an invaluable tool in not only getting information out to the public via a one-way communication, but it has been expediential in recruiting efforts. This site offers individuals the opportunity to email an officer directly with questions that mostly pertain to recruiting and details on how to become a police officer with HPD. This blog was recently voted on by a security system company as the Best Police Blog of 2012. It is engaging and contains not only videos but high resolution photographs of HPD in action.
- *YouTube* The department operates a YouTube channel, **houstonpolicedept**. The HPD Video Production staff uploads videos onto this site regularly. The public has the ability to view videos such as charitable events HPD has participated in, crime surveillance videos and the monthly media briefing with the Chief of Police regarding HPD issues, just to name a few.
- *Podcast* "HPD Reports" provides citizens with monthly updates on the department's events and activities.
- The department posts crime statistics on the HPD website, http://www.houstonpolice.org. The crime statistics page also includes a link to the "My City-Recent Crime" Web Mapping Application, http://mycity.houstontx.gov/recentcrime/index.html. This is a web-based mapping application that is designed to allow its users to view and search out recent crime data for the City of Houston. The recent crime data is pushed to the enterprise Geographical Information Systems (GIS) from HPD's database each morning.
- The department permits citizens to make reports of certain crimes through the internet, via the HPD website's Online Police Report service.
- The Houston Emergency Center (HEC) publishes "Active Incidents" for police and fire through the computer aided dispatch system. The Active Incidents are viewable at http://cbtcws.cityofhouston.gov/ActiveIncidents/HPDIncidents.aspx.

Conclusion

The utilization of social media is thriving amongst police agencies worldwide. It has become an additional resource, outside of local newspapers, television and radio stations, that allows agencies to reach out to the community and use the public as an investigative tool to help fight crime. As social media continues to expand and when implemented effectively, it appears that it has become a bigger factor as an investigative tool or for the reporting of crime.

Larry J. Yium
Digitally signed by Larry J. Yium
DN: cn=Larry J. Yium, o=Houston Police Department, ou=Deputy Director, email=Larry.Yium@cityofhouston.net, c=US
Date: 2013.01.25 10:48:05 -06'00'

Larry J. Yium, Deputy Director
Planning

ljy:moh

Planning Control #8541

Mark L. Curran
Digitally signed by Mark L. Curran
DN: cn=Mark L. Curran, o=HPD-Staff Services Command, ou=Assistant Chief, email=Mark.Curran@HoustonPolice.Org, c=US
Date: 2013.01.25 11:52:08 -06'00'

T.N. Oettmeier
Digitally signed by T.N. Oettmeier
DN: cn=T.N. Oettmeier, o=HPD, ou, email=Timothy.Oettmeier@houstonpolice.org, c=US
Date: 2013.01.25 13:01:26 -06'00'

Houston Police Department
Social Media Usage 2012

The Houston Police Department (HPD) currently has it's footprint within many social media outlets including, Twitter, Blogs, YouTube and most notably Facebook.

The HPD Blog was initially created in 2007 for recruiting purposes. It is used for announcing recruiting events, following cadets through the Academy, providing background and history of HPD and positive stories in general. The blog is still maintained to this date and currently receives around 2500 visits per day.

The Houston Police Department launched its Facebook page in August of 2009. Since its inception, it has become extremely popular with a fan base of more than 32,000 and grows daily. The site features positive news stories about the Department, crime fighting efforts and promotes community initiatives. In many cases, the media has created feature stories from information posted on the site. While the page is monitored by Public Affairs staff during business hours, after hours Command Center staff checks the site in the event that any inappropriate comments are made regarding postings on the site.

Also in 2009, HPD began "tweeting" on the micro blogging site known as Twitter. This one way communications tool for mobile phone users is used to alert citizens of street closures, weather alerts and potential dangers. Department Public Information Officers have also used the site to release information about breaking news, special events and highlights of Chief McClelland's monthly press briefings. Additionally, we link "tweets" to video and photos of wanted criminals to ask the public for help in locating dangerous criminals. The page has almost 3,000 followers to date and is growing on a daily basis.

HPD has had its own Youtube channel since December 2007 with 361 subscribers as of December 2012. The department has posted 171 videos, ranging from public safety announcements, coverage of press conferences, special events and media availabilities to educational crime prevention presentations. Special postings include surveillance videos and video news releases.

APPENDIX X

IACP CENTER FOR SOCIAL MEDIA

Supporting the Needs of Law Enforcement Online

The Social Media Beat

In Case You Missed It...

By IACP Center for Social Media

IACP Center for Social Media

IACP's Center for Social Media is a clearinghouse of information and no-cost resources to help law enforcement use social media.

Read Full Bio...

One of the challenges of working in the social media realm is that it is constantly evolving – new platforms become popular, new functions are added, and new terms are coined. In the last few weeks, there have been several big changes to the most popular social media platforms. In case you missed them:

Twitter Login Verification

On May 22nd, Twitter announced they have launched a two-factor authentication process to enhance account security and prevent unauthorized access. If enabled, you will need to enter a verification code that is sent to your phone via SMS to sign into your account. The code can only be sent to one cell phone so this may not be an ideal option for agencies that need to give access to multiple users.

Verified Facebook Pages

On May 29th, Facebook announced that it is beginning to verify pages and profiles. Similar to verified Twitter accounts, a small blue check mark will identify a verified page or profile. While this will take many months to completely roll out, we've been discussing the importance of verifying law enforcement accounts with Facebook staff. Stay tuned!

Twitter Lists

On May 30th, Twitter announced they have expanded the number of lists you can create (from 20 to 1,000) and the account cap per list (from 500 to 5,000). As a result of this change, IACP has added 50 new lists of law enforcement agencies on Twitter – one for each state! Check it out and subscribe to the lists at https://twitter.com/TheIACP.

LinkedIn Authentication

On May 31st, LinkedIn announced that they have launched two-step verification to add additional security measures to your account.

Facebook Hashtags

On June 12th, Facebook announced they are following the lead of other social media platforms by incorporating clickable hashtags. If you're not familiar with hashtags, they are a way to organize and search for content about a particular topic. An example of a hashtag that will get a lot of use in the coming months is #IACP2013.

To stay on top of changes like those described above, be sure to subscribe to our Items of Interest RSS feed to get daily updates on what's new in the world of law enforcement and social media.
Return TopTrackbackPrintPermalink
Popular tags: Twitter, Facebook, LinkedIn, Strategy, Privacy Safety and Security

Leave a Reply

Comments that include profanity or personal attacks or other inappropriate comments or material will be removed from the site.

Name (required)

E-mail (never displayed, shows your gravatar)

APPENDIX XI

The New York Times

March 28, 2013

Police Dept. Sets Rules for Officers' Use of Social Media

By J. DAVID GOODMAN and WENDY RUDERMAN

Looking to avoid troublesome social media postings by its officers, the New York Police Department has issued strict guidelines and ordered its members to comb through their personal profiles on Facebook, Twitter and other Web sites to ensure they are in line with the new rules.

As word of the order spread, police officers across the city checked their accounts to see if anything they had posted might run afoul of the new rules. Some edited their personal accounts to remove references to the department.

One officer, who had served in the military, replaced a Twitter profile photo of himself in his blue patrol hat with a portrait of himself in an Army uniform. Another wondered if his profile should include the word "detective."

For years, officers faced relatively few official restrictions on social media, where many proudly posted photos of themselves in uniform and listed their job as "N.Y.P.D." Indeed, the Police Department has lagged behind other jurisdictions in formalizing rules for personal online behavior.

"Such an order is not unexpected," said Roy T. Richter, president of the Captains Endowment Association, the union that represents high-ranking officers. "The only surprise is that the order was not put out before now."

The order followed recent embarrassing online activity at the Fire Department in which two of its members, including the fire commissioner's son, wrote racially inflammatory Twitter posts. Commissioner Raymond W. Kelly, however, said on Thursday that his order had been in the works long before.

The Fire Department is drafting its own social media policy, a spokesman said.

In issuing the new rules, Mr. Kelly sought to motivate officers to scrutinize their postings in what appeared to be an effort to defuse any lurking social media land mines.

The three-page order dated Monday details online behavior that could land officers in trouble, including posting photos of other officers, tagging them in photos or putting photos of themselves in uniform — except at police ceremonies — on any social media site.

Members of the department are also “urged not to disclose or allude to their status” with it. Doing so could make that person ineligible for certain sensitive roles.

Other regulations were more straightforward: Do not post images of crime scenes, witness statements or other nonpublic information gained through work as a police officer; do not engage with witnesses, victims or defense lawyers; do not “friend” or “follow” minors encountered on the job.

Violations of the order can result in disciplinary action, including dismissal. Officers with existing social media accounts are ordered to “immediately ensure that their personal social media site is reviewed and in compliance with this order.”

The order, which builds on the city’s general social media policy and was reported on Thursday in The Daily News, comes a year and a half after officers posted insulting Facebook comments about the West Indian American Day Parade. In that case, more than a dozen members of the department were disciplined.

It also barred local commanders from sending out posts without approval from the department. Last year, one Brooklyn precinct commander was criticized for posting photographs of men about to be released from custody to a Twitter account maintained by the precinct.

“I think the captain’s actions were actually another example of the innovative thinking of our precinct commanders,” Mr. Richter said on Thursday. “He was thinking outside the box and he should be commended.”

Mr. Kelly said the order was intended partly to avoid confusion between the department’s official statements on social media, and personal statements by officers. He likened the rules to those put in place by many other agencies and private businesses.

“One of the issues in a complex business like this is that people say they’re part of an organization, this organization, and make a statement that the public can interpret as policy,” he said. “You can’t run an organization like that.”

But, he said, the department had not assigned anyone to comb through social media sites looking for violations; the new rules would be enforced when the department learned of potentially troublesome postings.

The guidelines appeared to broadly match those adopted by other big city departments around the country.

The Detroit Police Department issued its guidelines in 2011 after an officer posted photos of a suspect wielding a machete on his Facebook page. That same year, the Albuquerque police also barred department members from identifying themselves on social media. That order came shortly after an officer, involved in a fatal police shooting, was seen on Facebook describing his job as "human waste disposal."

◀ OPEN

MORE ON THE HOME PAGE (1 OF 1

Egypt Crisis Finds Washington Largely Ambivalent and Aloof

Read More »

APPENDIX XII

Social Media Elevates Community Policing

Interactive with the Community

BY: Indrajit Basu | August 6, 2012

Picking up a tip or two from tech-savvy children is not unusual these days for parents living in an increasingly connected world. For Newberry County, S.C., Sheriff James Lee Foster, however, a tip from his children not only helped his department solve crimes more quickly, it also helps him stay plugged into his community like never before.

Following a tip from his children, Foster put his department on social media and has been getting daily tips on county crime information. He said that the community has taken up the idea so well that he had to open multiple pages in Facebook to beat the social network's built-in friend limit.

Newberry County is one example among many places where social media is changing how police work is done. "The exponential growth and popularity of social media and its effectiveness of communicating with a community is helping law enforcement departments across the U.S. to redefine what community policing is," said Nancy Kolb, senior program manager, at the Virginia-based International Association of Chiefs of Police (IACP) Center for Social Media.

"Social media is not only helping community policing rise to a new level, it is also helping the police to directly engage citizens," Kolb said.

While some law enforcement agencies have already experienced "tremendous success" with the adoption of social media, many more are coming on board.

According to IACP's latest social media survey, 40 percent of agencies in the U.S. are already using platforms like Facebook, Twitter, YouTube and the like to solicit tips. Most others -- 80 percent according to the IACP survey -- use social media in some capacity.

The fact is that the advent of social media is having a huge positive impact on local police efforts.

Hubbard, Ohio, city police, for example,adopted social networking sites, like Facebook and Twitter, and began receiving important information from the public.

According to Sgt. Howard Haynie, who helps monitor the department's Facebook and Twitter pages, tips and information gathered from these two social sites helped the department to solve two different crimes within a two-week span.

It's a lot of help for a small department like Hubbard city police, said Sgt. Haynie, who believes that social media is emerging as a force multiplier for the department.

It's not all about crime solving, though. Mark A. Marshall, president of IACP, is enamored by social media's engagement power. "It allows law enforcement leadership to humanize their work and their officers, disseminate information, and directly engage with citizens through the online communities in which they participate," Marshall said.

"Social media's biggest benefit [for law enforcement] has been the daily interaction between the department and the citizens. It has allowed the department to provide more of a personal approach to its services," said Lynn Hightower, communications director of the Boise, Idaho, Police Department (BPD).

BPD began utilizing social media tools as part of its communication strategy around 2009, when -- driven by the explosive popularity of social media -- officials saw an opportunity to communicate with a larger and more diverse demographic.

Hightower said after thorough research she decided upon the most popular and growing sites where they could get “the most bang for their buck.”

The Boise PD started with Facebook, and has included Twitter, Nixle, and YouTube in its social media strategy as well.

“Obviously social media does not always help us in solving crimes. But it has helped us improve relationships, help build partnerships that make the department more effective in the primary mission,” Hightower said.

“A few days ago I put out a tweet on proper fitting of car seats for children. Unexpectedly this simple post escalated into a major discussion involving 45 conversations with 6 people -- and eventually it turned into a discussion that impacted a citizen’s safety,” she said. “Without that tweet our residents would never had the opportunity for reach out to the Police Department for an answer to that issue.”

The Boca Raton, Fla., Police Department (BRPD) has taken the application of social media for law enforcement a step further.

Realizing that the perks of using social media channels are often much bigger than only relaying crime reports, crime tips, and traffic updates, BRPD now uses the medium mainly for disseminating information.

”The media doesn’t cover the local communities like they used to. It has to be a bigger story for press , so the residents do not get to know about the little stories about crime, and what’s being done about it,” said Mark Economou, public information manager for the BRPD.

“A lot of information passes through the social media before it reaches other channels, and we realized that it is imperative for police departments to have a presence there,” Economou said.

Economou added that the BRPD social media (Facebook and Twitter) is a two-way channel for discussing and sharing crime info between the public and its Police Department. Additionally it also uses social media (Nixle) to provide immediate information via text or e-mail during an emergency situation.
It’s all about serving citizens, said the police department representative interviewed for this story.
“The prerequisite to a successful and effective police department is public confidence and trust. Social media helps a (police) department to earn that trust,” said Hightower.

Clearly then, social media is here to stay. It has revolutionized the way citizens communicate with public safety agencies as well as each other.

While there is no single right way to use social media, Hightower’s most important tip for an effective social media practice is; “be useful, be relational and be reliable.”

This article was printed from: **http://www.digitalcommunities.com/articles/Social-Media-Elevates-Community-Policing.html**

APPENDIX XIII

stltoday.com
the #1 St. Louis website

Online networks link neighbors, can help fight crime in St. Louis area

FEBRUARY 23, 2013 2:30 PM • BY KIM BELL
KBELL@POST-DISPATCH.COM 314-340-8115

Nancy Casey wasn't sure how to connect with neighbors in her sprawling O'Fallon, Mo., subdivision after a few burglaries in the area.

Her family moved to the Homefield subdivision about eight years ago from a military base, and she says it was hard to get used to a neighborhood that didn't have the unifying force of a shared military structure.

After the burglaries, police gave her a packet of information about an upcoming National Night Out anti-crime event. Inside she found a solution to the disconnected nature of the suburban area. The packet mentioned the social networking site Nextdoor, a way to link up neighbors online.

She set up a site for her neighborhood in July, and Nextdoor is paying to send out 50 postcards a month to residents to tell them about the site. Scores of families have joined.

Nextdoor and a similar, competing site called i-Neighbors allow residents to set up social networks linked not by friendships or interests but geography. In a society in which fewer people really know their neighbors, the sites help people connect and can be a valuable tool to combat crime. In some places, police are actively working to get neighborhoods online to help share information and stifle criminal activity.

In Casey’s neighborhood, residents now have a way to communicate with one another if they see something suspicious or out of place. If they spot vandalism at the park, they don’t keep it to themselves. They post it to the site, and Casey springs to action to alert police and ask the maintenance crew to remove graffiti.

“It’s really working out, as far as communication,” Casey said.

On both Nextdoor and i-Neighbors, residents create a site for their neighborhood, then recruit others to join — with their real names and addresses. Both are free, though i-Neighbors recently launched a new service, for a monthly fee, which community leaders can use to broadcast text alerts to cellphones and send prerecorded voice messages in emergencies.

Members can post a photo of themselves and offer as much, or as little, information about themselves and their families as they want. Some people put up photographs of their front doors rather than photos of themselves.

Boths sites are becoming more popular in the St. Louis region, with about 100 neighborhoods using one site or the other by a recent count.

Keith N. Hampton, a sociologist who created i-Neighbors, said 75 neighborhoods within 25 miles of St. Louis have been active on the site in the past year. The sites are used by more than 120,000 people in 9,000 neighborhoods nationwide, according to the company.

Nextdoor, which launched nationwide in October 2011, says more than 70 neighborhoods have signed up to use its neighborhood websites in the St. Louis region. More than 8,500 neighborhoods are participating across the United States.

While some might think the computer is the lazy way to mingle with neighbors, Sarah Leary of Nextdoor says that people who connect online are far more likely to get together and meet their neighbors offline. The sites facilitate a desire to connect, she said.

“People have this interest in rebuilding a connection with their community,” she said. “That sounds like a nostalgic idea, but it really resonates.”

In some places, they are getting a nudge from police interested in the crime-fighting possibilities of the sites. In November, the Dallas Police Department announced it was partnering with Nextdoor to post crime alerts and information about crime trends that could be targeted citywide or to specific neighborhoods. About 100 Dallas police officers were trained to use the website. The company’s goal is to get 90 percent of Dallas neighborhoods to have a Nextdoor page within a year.

‘AN EARLY ALERT’

Mike Petetit, a resident of Lafayette Square and chairman of safety and security for Lafayette Square, said he hopes St. Louis will one day have Nextdoor citywide. He set up the site for Lafayette Square a few months ago and, with little effort, already has scores of the 777 households taking part. Petetit is also owner of the Park Avenue Mansion Bed & Breakfast and president of Neighborhood Ownership Model Inc.

Petetit's neighborhood also has three other user groups to share information. He'd like to eventually drive everyone to Nextdoor. He said the site works better than email lists, which can become swamped with spam. It also allows members to "mute" others they might find annoying, and create smaller subgroups around specific issues or concerns.

"In our neighborhood, we're already connected," Petetit said, "but this allows information to flow quicker."

Nextdoor also helps connect the neighborhood to police, who can get alerts when a resident wants to report something suspicious.

One resident used the site to remind his Lafayette Square neighbors to lock their car doors after a car break-in on Oct. 29. He told neighbors he saw three kids run off, with one stopping to ask for the time as a diversion. Such observations by members of the site can help police spot patterns or tie together incidents.

"It's fantastic," said St. Louis Police Officer Brian Min, the neighborhood liaison officer in Lafayette Square. "It's an early alert, something to keep an eye on."

And the site creates a personal connection. Residents might be more likely to send out alerts to an officer they know than to call 911 over something that might simply seem suspicious, Min said.

Plus, he said, "when you get people to communicate, it opens them up to develop a sense of community."

Indeed, while some use the sites to target crime, the sites are also used for other mundane things, like finding a baby sitter or plumber. Postings about missing pets are common in the St. Louis area.

Back in O'Fallon, Casey's adult daughter started chatting with another mom with children of the same age on the Nextdoor site. Soon they realized they lived within sight of each other but had never spoken.

"Now," Casey said, "they're arranging play dates."

Top of Page Home Full Site