Social Media Assessment

Deputy Commissioner Strategic Initiatives

4/22/2014

Contents

Introduction

This report is primarily based on a series of interviews with uniform and civilian members of the service (MOS) from nearly every bureau in the New York City Police Department (NYPD). The purpose of these interviews was to gather information on the Department's use of social media. In addition, we also spoke with a number of employeesin other police departments.

Prior to a discussion of NYPD social media use, in the first section, we examine NYPD policies related to the use of social media. Section 2 of this report describes how the NYPD disseminates information to the public using websites and social media assets. In Section 3, we assess the frequency and intensity of social media platform usage, and the typology of use for investigative purposes. Section 4 summarizes social media use at other police departments.Section 5 of this report provides a brief discussion of how the NYPD usesdigital platforms to collaborate internally. Finally, we provide recommendations in Section 6 and conclude this report in Section 7.

Section 1: NYPD Policies

There are no Patrol Guide Procedures related to the use of Social Media. There are two relevant Operations Orders. Operations Order # 34, entitled, "Use of Social Networks for Investigative Purposes – General Procedure" was issued on 09-15-2012 (Appendix 1). This order presents guidelines for using social media in order to conduct official investigations or research. The order particularly restricts use that requires an online alias which would conceal the user's true identity. Terrorism-related social media use involving an online alias requires approval by the Intelligence Bureau. All other online alias social media use requires the approval of the user's supervisor, commanding officer, and bureau chief or deputy commissioner. The order contains additional information regarding the federal Electronic Communications Privacy Act (ECPA), which describes legal steps for obtaining online account information from service providers.[1] The order concludes with notes regarding precautionary measures and Handschu guidelines.

Operations Order # 29, entitled "Use of Social Media by Members of the Service" was issued on 07-25-2013 (Appendix 2). This order governs official use of social media by members of the Department. Official use is governed by the New York City Social Media Policy, published by the Office of the Mayor. No member may post content to a social media site without the permission of the Deputy Commissioner of Public Information (DCPI). No member may establish an NYPD social media account without the permission of the Police Commissioner. All social media outlets currently used by the Department must be registered by MISD with the New York City Department of Information Technology & Telecommunications (DoITT). DCPI is responsible for all content posted on Department social media sites.

The order also restricts personal use of social media by members of the Department. Members are urged not to disclose their status as a member of the Department. Members are further prohibited from: revealing Department affiliations of other individuals; posting photographs of themselves in uniform or displaying official identification or equipment; posting nonpublic

[1] It should be noted that there are few court precedents related to the use of social media in investigations. In one 2012 case filed in the U.S. Southern District of New York, the Court held that the Government did not violate the Fourth Amendment when it accessed "private" information from a Facebook page (see http://www.x1.com/download/US_v_Meregildo.pdf).

materials that were gained as a result of their position with the Department; using a Department email address without the Police Commissioner's approval; making contact with witnesses, victims, or lawyers associated with an ongoing investigation or legal action; engaging in any type of social media contact with minors who are not family members.

In addition to these two Operation Orders, the Intelligence and Detective Bureaus have devised guidelines specific to their respective personnel. The Intelligence Bureau issued an internal document "Guide, Cyber Policies, Practices and Guidelines" in 2012 that creates operational and policy guidelines for Undercover Cyber Operations. The document includes specific information pertaining to how and when individuals can be engaged, how to create a fictitious account, and particular technological requirements (e.g., stand-alone computers). Information related to the inspection process and the requirements necessary to remain within Handschu guidelines are also included.Chief of Detectives Memo #27 (12-31-2012) expands on Operations Order #34 in order to address the specific requirements of the Detective Bureau.

Though not directly related to social media use, it should be noted that changes to the NYPD website are governed by Administrative Guide procedure # 322-38, entitled "Guidelines for NYPD Internet Website" (issued 6-01-2005). This guide discusses the process by which information is to be released by the Department for inclusion into the NYPD website (Appendix 3).

Section 2: Community Engagement

Websites

The official website is hosted by DoITT and is managed by the Management Information Systems Division (MISD).[2]MISD personnel report DoITT's technology is outdated, and that the NYPD is seriously constrained by the design and lack of control over content management on the site. Much of the information on the official website is buriedand some is outdated. For example, the information on Access to 911 for the Deaf and Hard of Hearing redirects you to a YouTube video that lists the Mayor as Rudy Giuliani and the Police Commissioner as Bernie Kerik.

The Department has approximately 15 other public facing websites (Appendix 4). Most of these websites, including CrimeStoppers, Finest Health and the Counterterrorism "Shield" site, are managed by MISD personnel. In addition, MISD manages the NYPD iPhone and Android mobile applications.

Social Media Accounts

The NYPD currently uses social media such as Facebook and Twitter to share information with the public about crime patterns, wanted persons, major events, and other matters.The Office of the Deputy Commissioner Public Information (DCPI) is responsible for all content posted on official social media sites (per Operations Order # 29).

DCPI is responsible for operating daily the official NYPD Facebook, Twitter, Instagram and YouTube accounts. At this time, there is one detective (Detective Scott Glick) assigned to do this. The NYPD Facebook page (facebook.com/NYPD) has over 200,000 followers, and the Department's Twitter account (@NYPDnews) has over 90,000 followers.

The Department has one YouTube account with several channels (InsideNYPD). The YouTube channel is primarily used to push out surveillance videos for wanted persons, explain certain

[2] Mayoral dictate under the Bloomberg administration.

police jobs, and provide information on community events. It has approximately 7,000 subscribers. InsideNYPDvideos have been viewed over 2,000,000 times.

Instagram has been actively used since January 2013. Since then, 198 photos have been posted to the Department's official account, OfficialNYPD. We utilize Instagram to share unique photos of personnel and vehicles, as well as share photos taken by the public that include the #NYPD tag in their post. The premise is to add positive photographs, both ours and the members of the public, including vintage NYPD moments and allows people to interact quickly and easily by "liking" the picture. The Department's Instagram account has 6,860 followers.

Beyond DCPI, personnel in four other Bureaus – the Community Affairs Bureau, Counterterrorism Bureau, Detective Bureau, and the Personnel Bureau – are actively working to engage the public via social media platforms.

Community Affairs Bureau

The Community Affairs Bureau (CAB) has two Facebook accounts. The first, the NYPD Community Connect page is for Precinct Community Council members who hold a position on the Executive Board (65 members). Members post events happening in their community, meetings times of their community council, and respond to requests for information. The Citizens Police Academy (CPA) page is for alumni of the Citizens Police Academy (139 members). Sgt. Keisha Ward (CO of the CPA) is informed of all membership requests for verification purposes. Approved members post event information, reunion information for specific CPA classes, and any other information relevant to the CPA. MOS assigned to CAB, DCPI and the Office of the Chief of Department (OCD) monitor both of these sites and engage if needed.

The Community Affairs Bureau also has a contract with "Constant Contact".This software provides CAB personnelwith the ability to manage their email address contacts (32,870 as of 2/26/2014). CAB personnel are able to build out selected mailing lists and send "blast" emails to contacts in specific neighborhoods/groups (Appendix 5). There is a "text2Join" capability

that allows users to join an email distribution list by text message. Metrics are built in (e.g., who opened the email). It should be noted that approximately 400 people have "opted out" of the email distribution list this year. One criticism is that the software does not have the capability to set email frequency preferences, which could potentially affect the "opt out" number.

CAB recently piloted a "virtual community council meeting" in the 112 precinct using an online service (spreecast). The response to the 112 precinct pilot was overwhelmingly positive. CAB personnel, the 112 Precinct Community Council President, and viewers felt there was value in having an online way to participate in the meeting. The software is no cost to the NYPD, though interested viewers (including MOS) are asked to provide specific information in order to sign up.

Of note, content management changes to the Community Affairs link on the NYPD website is the responsibility of one Police Officer assigned to CAB. MISD is notified of the requested edits, checks to determine the changes will not have an adverse technological effect, and publishes the changes.

Counterterrorism Bureau (Shield Unit)

The mission of NYPD Shield is to strengthen the Department's partnership with private security professional and to serve as the Department's program for communication with all private sector entities on matters of counterterrorism (Appendix 6). A separate and public and secured website was established in 2006 with multiple levels of access. There are approximately 13,000 members on the website (as of 2-10-2014). Content management changes are made by personnel assigned to the Shield Unit but must be approved by MISD. The Shield Unit uses software deployed by MISD"SmarterStats"for website metrics (e.g., daily report of unique visitors).

Detective Bureau(Crime Stoppers)

The Crime Stoppers website collects tips, shows wanted posters, and displays footage of crimes. As in CAB, personnel in Crime Stoppers have the ability to edit this site (e.g., upload videos and wanted posters). The Crime Stoppers program is supported by the Police Foundation. The Police Foundation distributes rewards and coordinates media campaigns to encourage public awareness.

Personnel Bureau (Recruitment Section)

The NYPD Recruit website, Facebook (NYPD Recruit), and twitter (@nypdrecruit) accounts are managed by a private vendor, the Bernard Hodes group. The NYPD Recruit Facebook page has approximately 34,000 followers and the twitter account has about 1,500 followers.Recruitment Section personnel use google analytics to monitor website and social media accounts usage.

The recruitment site is hosted on an easily maneuverable interface with live chat functions and mobile accessibility. Upon request, changes are quickly made to the site by the vendor. The Bernard Hodes group meets with the Recruitment Section regularly to discuss ways to improve the Personnel Bureau's brand strategy and marketing campaign. MOS in the Recruitment Section indicate they are pleased by the services provided by the Bernard Hodes group and feel the vendor does an impressive job using the platforms to "boost" NYPD recruitment ads and gain "likes."

Section 3: Investigative Use

The NYPD has members of the service in several Bureaus who analyze social media for investigative and intelligence purposes.Information from online sources such as Facebook,YouTube, Instagram, and Twitter is used to identify unknown suspects and criminal networks, collect evidence and to look for potential criminal and terrorist threats.

As previously noted, the use of social media for investigative purposes is governed by the guidelines set forth in Operations Order #34. Many investigations are conducted using NYPD computers on the Department network.However, it should be noted that due to slow connection speeds, lack of field devices, and lengthy approval processes, many MOS reported using their own personal computers and handheld devices.

MISD is responsible for managing internet content filters for the Department. Specific permission has to be granted for access to particular categories of information on the internet (e.g., social media sites). At this time, a 49 to DC OIT through the appropriate channels is required to gain access to social networking sites. In some situations, MOS may believe particular sites are in the social media category. However, they may not be categorized this way by MISD. Alternate permissions may need to be granted. For example, hoodup.com is categorized as "adult content" so the requestor would not have access without requesting this type of permission.

Counterterrorism Bureau

Terrorism Threat Analysis Group

The Terrorism Threat Analysis Group (TTAG) uses social media platforms to monitor and report online Jihadist activity. The TTAG focuses primarily on forums, websites, blogs, chartrooms, Twitter and Facebook. TTAG's products are disseminated in the Jihadist World Weekly report. This report is given to U.S. law enforcement partners, intelligence agencies, and the military.

Precautions are taken to ensure that the NYPD's investigations on these sites remain untraceable. As part of these precautions, TTAG does not engage any users on these forums.

When data is collected from these platforms the interests of other law enforcement and intelligence agencies are considered. The Counterterrorism Bureau is primarily interested in information, discussions, and media content pertinent to various aspects of terrorist tradecraft.

Personnel Bureau

Applicant Processing Division

NYPD applicants are required to list all social media accounts as part of the NYPD application process. In addition, during the review process, applicants are required to login to their social mediaaccounts and allow investigators to review the content. In January 2013, a bill was proposed on the City Council Floor that would allow the applicants to refuse this request without "discharge, discipline or penalty" (Appendix 7). Assistant Commissioner Susan Petito had worked with the Law Department to create some amendments, putting in a law enforcement hiring exception, but the bill ended up not going forward, so it was never amended to include the exception. It is possible this bill will be re-introduced in the Council in 2014 and could potentially hinder the NYPD background investigation process. There arealso a couple of pending State bills that are similar in nature (Appendix 8). The NYPD is on record opposing the State bills as written because of the same concerns.

Detective Bureau (Computer Crimes Squad)

The Computer Crimes Squad (CCS) is responsible for providing investigative support for computer and digital / multimedia evidence related crimes both proactively and through forensic examination where a computer or other digital / multimedia device is involved.CCS conducts forensic examination and analysis when necessary of all digital / multimedia evidence including but not limited to the following: Desktop Computers, Laptop computers, Tablets, Game consoles, Smart phones, Cell phones, MP3 Players, Personal Organizers, GPS Devices, Internet Routers and Digital Video Devices (Cameras, DVRs).

They provide advice and assistance (including responding to an incident scene) regarding the recognition, identification, documentation, processing, collection, evaluation, examination, analysis, etc., of digital / multimedia evidence. CCS responds to crime scenes to conduct digital triage forensics and other necessary functions. They provide support and technical assistance when tracking suspects wanted in connection to a crime, missing persons, and all other appropriate circumstances when they are known to be using specific computers, digital / multimedia devices and/or internet accounts (ex. Email Accounts, Social Networking Accounts, etc.)

CCS also conducts criminal investigations involving Cyber Security incidents and events. They receive cases strictly on a referral basis (e.g., from Squads, CrimeStoppers, directly from Facebook, community members).For investigative purposes, the Computer Crimes Squad has its own server (Apple XM) that is not connected externally (black server/black network).

The Computer Crimes Squad is the designated the lead agency representative and coordinator for the Department of Justice New York City Internet Crimes Against Children (ICAC) Task Force, which is comprised of Federal, State and Local law enforcement agencies.

The Computer Crimes Squad is a recipient of the Department of Justice,Office of Juvenile Justice and Delinquency Program,Internet Crime against Children Program Support grant. They use these funds for training, software, and equipment.

Internal Affairs Bureau

Any action taken by a police officer (on or off duty) may be reported on a social networking site, and in some cases, actions are recorded and uploaded for the public to hear/view. The Internal Affairs Bureau (IAB) has responsibility for these cases. MOS assigned to IAB noted that most of their work is reactive. For example, someone will call and say that their neighbor (a MOS) is posting inappropriate content on Facebook. Since “friending” the MOS would raise suspicion, IAB often asks the reporter to allow them access to their own social networking site so they can monitor content without raising suspicion.

Intelligence Bureau

There are two units in the Intelligence Bureauprimarily focused on social media - theSpecial Activities Unit and the Cyber Intelligence Unit. In addition, many Field Intelligence Officers in precincts throughout the city (especially those embedded with SET teams) use social media for investigative purposes.

Special Activities Unit

The Special Activities Unit is a 24/7, real time investigative support unit tasked with open source intelligence collection and analysis from online sources and social media.Through the use of open source cyber searches and social media platforms such as Facebook, Twitter, and other websites, SAU monitors the internet for indications of past crimes as well as crimes that may occur. SAU also searches the web for indications of disruptive events such as large unpermitted/unscheduled demonstrations within New York City and street parties/raves/flash mobs. Additionally, the unit monitors for threats to public officials, including the Mayor and Police Commissioner, threats to New York City, and other activities of interest to the Department. Investigators also make efforts that allow for social engineering, data mining and predictive analysis. SAU uses covert laptops on an Amazon wireless service (purposefully different than the Cyber Intelligence Unit).

Cyber Intelligence Unit

Uniformed members and analysts within the Cyber Intelligence Unit (CIU) monitor potential terrorist and criminal threats to New York by viewing publically available information in online internet forums, social networks, and other websites. Analysts and Detectives locate and access this information through open sources and via the establishment of profiles on the appropriate websites, or via subpoena results obtained from the website hosting company. CIU also supports criminal and Handschu-authorized terrorism investigations covertly, through the use of Cyber undercover officers. CIU uses covert laptops with air cards. Each member of the Unit has a number of different identities, which are shared with federal agencies. CIU has created and delivered in-house cyber training programs to various members of the service assigned to the Intelligence Bureau.

Community Affairs Bureau (Juvenile Justice Division)

In 2006, MOS began using social media to identify crews and map out crew territories in Manhattan. This eventually led to the establishment of the Juvenile Justice Division (JJD)in 2012. Currently led by AssistantCommissioner, Kevin O'Connor, MOS assigned to JJD use social networking to gather information on crimes committed by youthful offenders in neighborhood crews throughout the city. A number of MOS (especially SET teams) rely on JJDto conduct social media investigations on their behalf. JJD has trained FIOs and SET teams on how to move through social media pages, "friend"crew members, and monitor social media accounts.

Organized Crime Control Bureau

NarcoticsDivision

The Narcotics Divisionprimarily relies on Facebook to identify subjects andmake connections among people/groups. They also focus on craigslist, as illegal drugs can be purchased from this site. That said, the majority of cases they have been able to build using craigslist involve marijuana, which calls into question the benefit of exerting the effort required to make a case this way. In addition, most craigslist cases are time consuming and often lead to another precinct or patrol borough, making these types of cases more difficult as the Narcotics Division issued an internal memo that precludes UMOS from conducting cases outside of their geographical area. It was suggested that a dedicated citywide team that was allowed to cross boundaries might be more effective in shaping social media cases.

Many of the UMOS, including undercovers, utilize their personal computers/handheld devices to go on social media sites. It was also noted that some of the potentially more serious criminals rely on sites (e.g., hoodup.com) that are not categorized by MISD as social media, thus requiring alternate permissions to access.

GangDivision

Gang Division personnel rely heavily on social media. They currently have about 15 major cases and using social media assets for at least 10 of these investigations. They primarily rely on

Facebook but noted that Twitter has been useful in determining what other social media accounts an individual has. Gang Division personnel indicated that Facebook sites have been particularly useful in determining when best to serve a warrant (e.g., some individuals post everything, including when they are at home in bed).

The Gang Division conducts three types of queries: 1) passive queries of open source information, 2) passive queries of private accounts when a confidential informant gains access to a private page, and 3) active engagement. Gang Division uses registered confidential informants to gather information on private pages.

Gang Division personnel use department computers, department issued Samsung tables (have 6, 12 to 18 on order), and personal devices. The Gang Division uses Facebook's law enforcement portal to preserve pages for 60 to 90 days.

Vice EnforcementUnit

The Vice Enforcement Unitis responsible for investigating human trafficking and child pornography cases. Many cases are self-initiated. They noted that while some suspects are using social media platforms such as Facebook and Twitter, a number of individuals are using online dating services (e.g., Meet24.com). In addition, many are still using online services such as internet chat rooms (AOL, Yahoo) to commit crimes. Vice investigators engage these individuals using different personas (e.g., pretend to be a 14 year old girl). Many of the individuals want to engage using webcams; this is problematic due to the lack of undercovers. They have one physical undercover that can be used when it is necessary to meet. It was noted that other police departments have actually set up fake bedrooms.

Vice conducts investigations on department computers. They also have two non-NYPD computers connected to a wireless modem service provider (Time Warner Cable) for more sensitive cases. They also utilize their own personal devices, and report this becomes an issue for courtroom purposes. Vice is using Google Voice. This service allows the user to text and make phone calls from their existing phone number but will appear as a different phone number or area code of your choice to the subject. The biggest benefit to this program is that you can text from a computer, your phone, or any device that allows you to download

applications. The texting is stored on the Google Voice server, and can be viewed simply by logging into your email. They report Google Voice has been helpful, as they are able to document conversations in an efficient and professional manner (as opposed to taking screen shots off phones).

Other Commands

MOS in the Patrol Services Bureau, Detective Squads, the Housing Bureau, and the Transit were surveyed by their parent commands for this assessment. Generally speaking, they use social media in similar ways, though the actual level of use varies by command. PSB and HB access is usually limited to Special Operation Lieutenants and Field Intelligence Officers, and some Precinct and PSA commanders personally monitor social media.Precincts with SET teams (32, 44, 67, 73, 113, and 120) appear to use social media more than the others; this is unsurprising given the focus of SET teams is to monitor crews. In Transit, the Graffiti Unit appears to rely on social media the most.

Monitoring is both proactive and reactive.Commands noted social media enables them to identify upcoming house parties, look for pending acts of retaliation, and helps to better deploy personnel (e.g., Impact Response Team). Commonly used social media platforms include Facebook, Twitter, YouTube, Instagram,Pinterest, LinkedIn, Kick, WorldstarHiphop, Craigslist, and Sound Cloud. Many of the MOS have received no formal training, though some mentioned they have attended JJD seminars.

In sum, there is likely duplication among some of the investigative work being conducted in these bureaus/units, the exception would be in the Intelligence Bureau's Cyber Intelligence Unit and the Vice Enforcement Unit.

For the most part, their efforts seem to be compartmentalized, potentially leading to redundancies and lack of coordinated investigations. With the exception of individual relationships or contacts within these bureaus, systematic efforts are not made to coordinate their resources.

Training

Social media training is disparate and potentially offers conflicting information. The Department has no enterprise wide formal set of training seminars. The Training Bureau's Executive Development Unit (EDU) has offered a number of Social Media Related Courses since 2008 (Appendix 9). The Juvenile Justice Division has prepared their own training seminars and delivered them to various personnel throughout the Department. The Intelligence Bureau has its own internal training sessions.

MOS appear to be continuously looking for external training options and noted a number of external trainings they have attended. The Manhattan District Attorney's Office occasionally offers trainings. The Internet Crimes against Children Task Force (http://www.icactraining.org/) offers several training. Some of the ICAC trainings are "Undercover Chat Investigation Training", "Gigatribe Training", "Child Protection System Training", "Ares Training", "Bittorrent Training" as well as other local forensic trainings regarding data recovery.

The National Center for Missing and Exploited Children also holds trainings throughout the country regarding internet crimes against children. MOS have attended their "Forensic Imaging" training, which offers age regression and progression techniques, and apply to the use of undercover photographs during the chat cases and allows us to alter the images making the UC look slightly different or younger.

Other trainings mentioned include those offered by the:Hetherington Group (www.hetheringtongroup.com); Charles Cohen, Cohen Training and Consulting, (www.issworldtraining.com), and the National White Collar Crime Center (NW3C) (www.nw3c.org).

Section 4: Social Media Use at other Police Departments

A recent DCSI survey of social media use by other police departments included the following agencies: Los Angeles Police Department, Chicago Police Department, Philadelphia Police Department, District of Columbia Metropolitan Police, Houston Police Department, Virginia Beach Police Department, and Burlington (VT) Police Department. These departments spoke to us informally about their policies and prohibitions, as well as their day-to-day practices with social media.

All seven agencies place similar restrictions on off-duty use of social media by employees. These restrictions include: discussing official or confidential department business; uploading department materials or materials gained through employment with the department; identifying other department employees; implying official department endorsement of a product or service; and posting communications that discredit or reflect poorly on the department. Some agencies prohibit their employees from posting images of themselves in uniform or with similarly identifiable equipment; in several cases, such equipment includes firearms.

Similarly, all seven agencies use some combination of Facebook, Twitter, and other social media platforms to alert members of the public to matters of interest. In practice, these communications are similarly straightforward in content and style – alerts regarding traffic conditions, missing persons, wanted persons, and extreme weather advisories, for example. In addition, some agencies use Facebook to post press releases and human-interest stories. More than one agency posts messages regarding its K-9 unit's dogs.

A few of these agencies have formal guidelines regarding official use of social media. The guidelines are similar across agencies. They distinguish between using social media in overtly official ways and using social media surreptitiously for the purposes of investigation. The agencies which have formalized policies identify processes for approving the content of posted material, with authority usually resting with the department's commissioner or superintendent,

but approval is generally delegated to the agencies' media/public relations offices. Each department requires its employees to abide by municipal rules regarding computer use.

Of the seven agencies surveyed, Philadelphia Police Department's (PPD's) use of social media deserves comment. PPD's use of social media is deliberately eccentric and playful. PPD is making a conscious effort to attract the attention of people who do not generally follow police Twitter feeds. To do so, PPD posts witty, lighthearted, or occasionally irreverent messages that are intended to attract broad attention and keep it. PPD supplements these humorous posts with wanted photos, missing persons alerts, and crime- or police-related messages; these messages reach a wide audience that is actively paying attention to PPD posts. PPD has decided that its official messages reach more people because they are essentially piggy-backed on its other offbeat posts. The director of PPD's social media program has called this style a Trojan-horse approach to gaining and retaining broad public interest and engagement.

In addition to PPD's official Facebook and Twitter feeds, PPD has trained and authorized three to four dozen officers to make informal Twitter posts, from verified Twitter accounts which identify them as PPD officers. These Twitter officers are of all ranks and assignments, and their posts span a wide range from official and direct to irreverent and unrelated to police work – as do their responses to followers' comments. Here again, PPD's objective is to gain as large a social media following as possible, and each Twitter officer attracts followers for different reasons. All Twitter officers, however, weave official police-related information – especially wanted photos and descriptions – into their posts. In a deliberately indirect way, this information reaches a wide, engaged audience.

The International Association of Chiefs of Police (IACP) recently released the results of their 4th annual social media survey. Five hundred law enforcement agencies participated in this survey. The survey highlights[3] are as follows:

- 95.9% of agencies surveyed use social media.

[3]See http://www.iacpsocialmedia.org/Resources/Publications/2013SurveyResults.aspx

- The most common use of social media is for criminal investigations at 86.1%.
- The most frequently used social media platforms are Facebook (92.1%), Twitter (64.8%), and YouTube (42.9%).
- 57.1% of agencies not currently using social media are considering its adoption.
- 69.4% of agencies surveyed have a social media policy and an additional 14.3% are in the process of crafting a policy.
- 80.4% of agencies report that social media has helped solve crimes in their jurisdiction.
- 73.1% of agencies state that social media has improved police-community relations in their jurisdiction.

Section 5: Digital Collaboration

At present, the Chief of Department's "best practices" website (SharePoint 2007) is the only mechanism through which MOS assigned to different Bureaus collaborate digitally. This site went live in July 2013 and is accessible to UMOS in the rank of Captain or above, Special Operations Lieutenants, and Integrity Control Officers.

As stated on the site, the purpose is "to take information sharing to another level" and "to combine our ideas and experiences into effective strategies." MOS working in the Office of the Chief of Department (OCD) post a variety of topics on the site (e.g., Enhanced Community Relations) in an effort to foster discussion among Commanding Officers and Executives. Currently there are over 150 open topics for discussion. Instructions on how best to use the site have been discussed during the past few Compstat meetings.

Section 6: Recommendations

The recommendations given in this report are based on specific noted areas for improvement.[4]

NYPD Website

- The official public website (ny.gov/nypd) is outdated. Content management changes necessitate going through a lengthy and unnecessary administrative change process. We should determine what steps need to be taken with DoITT to remedy this situation, or alternatively, consider decommissioning this website.
- Consider alternate internal content management approaches. At present, content management is haphazard and either dependent on MISD, personnel in specific Bureaus, or both.
- Consider hiring an e-commerce marketing team that can position our websites for success and work with OIT to build new sites (e.g. for Applicant Processing and the Training Bureau).

Social Media Strategy

- Develop a comprehensive social media strategy for the Department. Examine the current role of DCPI and MISD as part of this action plan.
- Consider expanding exactly who in the Department can use social media on behalf of the organization (e.g., designated "tweeters"). Keep in mind that not everyone is comfortable or interested in using social media; as such it may not be beneficial if this should become just another add-on to existing duties.
- Consider collaboration platforms related to social media use. For example, how can we internally share information regarding changes to what social media sites particular people are using.
- Research additional grant funding opportunities.

[4] Note: In 2011, the Executive Development Unit published a 49 with a number of recommendations for the development of an NYPD social networking policy (Attachment 10).

Access

- Review and consider streamlining the current process to obtain social media (or other) access on department computers.
- Make it clear which sites require particular types of access (e.g., Hoodup.com requires adult content access).

Staffing

- Not surprisingly, personnel issues were mentioned as a concern by nearly every person interviewed. Two units in particular, the Computer Crimes Squad and the Vice Enforcement Unit, stood out as the most in need of staffing increases. Consider a larger team dedicated to Internet Crimes against Children.
- It was noted that many MOS are unaware of what to do when they come across a child pornography or sex crime case. This information should be distributed more widely, especially at the precinct level – similar to GLA (If you have questions about GLA, call XXXX).
- A lack of digital undercovers (cyber vs. physical) is an issue in many commands (esp. Vice). Consider tools that offer "digital CI's" (see http://abcnews.go.com/m/story?id=20792348)
- Consider a cyber "working group" comprised of MOS from the various units using social media for investigative purposes (e.g., Juvenile Justice Division, the Intelligence Bureau, Computer Crimes, and Vice Enforcement). This working group could meet to discuss various best practices, training issues, and so on.
- Consider the feasibility of creating a single integrated cyber command, where resources could be shared across Bureaus.

Devices and Tools

- A number of tools are being used, or tested, in the Department (e.g., Radian6, iSaga, Spokeo, SnagIt, Camtasia, SmarterStats).
- Determine who and exactly which products are currently being used or tested. Conduct a cost/benefit analysis of each. Determine how to make these tools available to all MOS in need of particular products.
- Evaluate devices that can be used in the field so that Police Officers are not using their personal devices.

Training

- Consider the range of available training courses (internal and external).
- Determine who in the Department needs what particular type of training, and examine who (internally or externally) is able to offer it.

Education

- Consider current educational/outreach programs. For example, how can we educate children throughout the city about persons recording and selling information obtained online (e.g., Webcam).

Appendix 1

Note: Double Click to open full version

OPERATIONS ORDER

SUBJECT: USE OF SOCIAL NETWORKS FOR INVESTIGATIVE PURPOSES – GENERAL PROCEDURE	
DATE ISSUED:	NUMBER:
09-05-12	34

1. 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.

2. 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:

PURPOSE To conduct social network-based investigations and research.

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.

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:

Appendix 2

Note: Double Click to open full version

OPERATIONS ORDER

SUBJECT: USE OF SOCIAL NETWORKS FOR INVESTIGATIVE PURPOSES – GENERAL PROCEDURE	
DATE ISSUED:	NUMBER:
09-05-12	34

1. 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.

2. 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:

PURPOSE To conduct social network-based investigations and research.

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.

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:

Appendix 3

Note: Double Click to open full version

ADMINISTRATIVE GUIDE

Section: Records and Reports		Procedure No: 322-38	
GUIDELINES FOR NYPD INTERNET WEBSITE			
DATE ISSUED: 06/01/2005	DATE EFFECTIVE: 06/01/2005	REVISION NUMBER:	PAGE: 1 of 2

PURPOSE To expedite and coordinate the preparation, collection and approval of all Internet-related information.

PROCEDURE Whenever information is to be released by the Department for inclusion into the NYPD website on the World Wide Web:

BUREAU CHIEF/ DEPUTY COMMISSIONER

1. Designate a coordinator to oversee project.

NOTE *Coordinators will be identified for each subordinate command and will periodically hold meetings to discuss the bureau or deputy commissioner's individual site.*

COORDINATOR

2. Forward material being considered for inclusion onto the Department's website to the bureau chief/deputy commissioner for written endorsement of approval.

BUREAU CHIEF

3. Forward endorsed approved material to the Office of the Deputy Commissioner, Public Information.

DEPUTY COMMISSIONER PUBLIC INFORMATION

4. Forward endorsed approved material, to the Office of the Chief of Department.
5. Coordinate periodic meetings with Management Information Systems Division and coordinators to discuss submissions and implement individual plans.

CHIEF OF DEPARTMENT

6. Review material submitted and, if approved, forward with endorsement, to the Deputy Commissioner, Public Information.

MANAGEMENT INFORMATION SYSTEMS DIVISION

7. Assume responsibility for technical advice, in implementing each submission onto the website, after the Deputy Commissioner, Public Information has granted approval.

DEPUTY COMMISSIONER PUBLIC INFORMATION

8. Review, approve and submit proposed Internet material to the First Deputy Commissioner and Police Commissioner for their approval.

NEW • YORK • CITY • POLICE • DEPARTMENT

Appendix 4

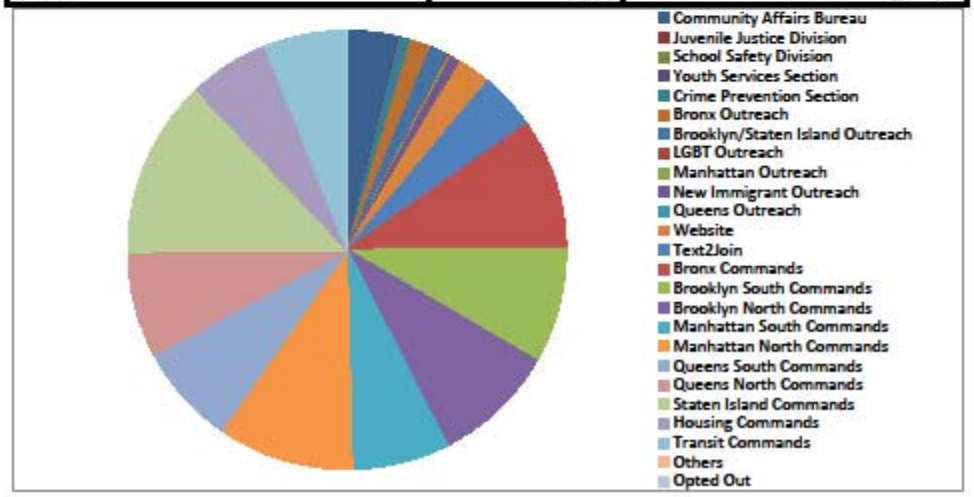
Source: MISD (As of Dec, 2013)

External Sites	Address
Primary Public Website	www.nyc.gov/nypd
Crime Stoppers	www.nypdcrimestoppers.com
Finest Health	www.nypd2.org/fh
Retiree Site	www.nypd2.org/retirement
Recruitment Site	www.nypdrecruit.com
Counter Terrorism Site	www.nypdshield.org
WTC resources	http://www.nypd2.org/fh/html/wtc_resources/Home.html
NYPD Equipment Store	https://www.nypdequipment.com/login.php
iPhone Mobile App	https://itunes.apple.com/us/app/nypd/id387943117?mt=8
Android Mobile App	https://play.google.com/store/apps/details?id=com.nypd.phonegap2&hl=en
WTC Health Questionnaire	https://a036-crimestoppers.nyc.gov/wtc_questionnaire/index.cfm
PC Sports League	http://www.nypd2.org/pcsportsleague/home.html
Cadet Program Info	http://www.nypdcadets.com/
NYPD Trainees	http://www.nypdtrainees.com/collegecredits.asp
School Safety Careers	http://www.nypdcivilianjobs.com/schoolsafetyjobs/
Social Media Accounts	
YouTube	http://www.youtube.com/nypd
Facebook	https://www.facebook.com/NYPD
NYPD on Twitter	https://twitter.com/NYPDnews
Commissioner Bratton on Twitter	https://twitter.com/commissbratton
Instagram	http://instagram.com/officialnypd
Internal Sites	
Intranet	http://finest
Enterprise Portal	http://portal
New Enterprise Portal Beta Version	http://betafinest
New Collaboration Sites	http://s1ppspdev01/sites/Collaboration/SitePages/Community%20Home.aspx
PMO Team Site	http://teams/sites/pmo/default.aspx
Chief of Department Team Site	http://teams/sites/ocd/default.aspx
Chief of Department Projects Team Site	http://teams/sites/ocd_proj/default.aspx
Community Affairs Projects Team Site	http://teams/CommunityAffairsProjects/default.aspx
Community Affairs Intranet Team Site	http://teams/CAB/default.aspx - Community Affairs Team Site (Portal)
COMPSTAT Team Site	http://teams/sites/compstat/default.aspx - COMPSTAT Executives Collaboration Site
Legal Matters Subpoena Team Site	http://teams/sites/dclmsubpoena/default.aspx - DCLM Administrative Subpoena team site
DCPI Team Site	http://teams/sites/DCPI/default.aspx - DCPI Team Site (being developed)
EMD Team Site	http://teams/sites/emd/default.aspx - Personnel Bureau Employee Management Division team site
Grants Team Site	http://teams/grants/_layouts/viewlsts.aspx - Grants Development Unit team site
OIT Team Site	http://teams/sites/ISO/default.aspx - OIT Information Security Office team site
Training Team Site	http://teams/sites/training/default.aspx - Training Bureau Portal
Transit Team Site	http://teams/sites/transit/default.aspx - Transit Bureau Team Portal
OMAP Team Site	http://teams/sites/omap
Department Manual Team Site	http://teams/sites/omap/mods/default.aspx

Appendix 5

Note: Double Click to open full version

CURRENT STANDINGS: EMAIL ADDRESS CONTACTS COLLECTED		
Email Signup Form	February 26	2014
Division Responsible	**28-Day Period**	**Overall Total**
Community Affairs Bureau	431	3870
Juvenile Justice Division	0	19
School Safety Division	0	147
Youth Services Section	18	46
Crime Prevention Section	95	329
Bronx Outreach	175	191
Brooklyn/Staten Island Outreach	156	202
LGBT Outreach	11	15
Manhattan Outreach	20	247
New Immigrant Outreach	89	212
Queens Outreach	0	39
Website	278	1391
Text2Join	481	880
Bronx Commands	1104	1679
Brooklyn South Commands	983	1729
Brooklyn North Commands	1040	1287
Manhattan South Commands	824	1298
Manhattan North Commands	1159	1773
Queens South Commands	849	1529
Queens North Commands	893	1383
Staten Island Commands	1509	2602
Housing Commands	681	1265
Transit Commands	696	1130
Others	0	10026
Opted Out	-3	-419
Total	**11489**	**32870**



Appendix 6

Note: Double Click to open full version

NYPD SHIELD Program

Appendix 7

Note: Double Click to open full version

Proposed Int. No. 1106-A

By Council Members Palma, Williams, Rose, Mark-Viverito, Foster, Nelson, Rivera, Koslowitz, Mendez, Rodriguez, Koppell, King, Dromm, Van Bramer, Lander, Brewer, Weprin, Gentile and Halloran

A Local Law to amend the administrative code of the city of New York, in relation to online social media and other personal online accounts and employment.

Be it enacted by the Council as follows:

Section 1. Subdivision e of section 2203 of the New York city charter is hereby amended to read as follows:

(e) The commissioner shall have all powers as set forth in chapter 8 of title 20 of the administrative code relating to the receipt, investigation, and resolution of complaints thereunder regarding earned sick time and confidentiality of online social and networking media and other personal online accounts.

§ 2. Title 20 of the administrative code of the city of New York is amended by adding a new chapter 8 to read as follows:

Chapter 8

Right of employees and prospective employees to confidentiality of online social and networking media and other personal online accounts.

§ 20-911 **Definitions**. For purposes of this chapter, the following terms shall be defined as follows:

a. "Employee" shall mean any person who is employed by any employer in return for the payment of direct or indirect monetary wages or profit, or any person who volunteers his or her services to such employer for no monetary compensation.

b. "Employment agency" shall mean any person undertaking to procure employees or opportunities to work.

Appendix 8

Note: Double Click to open full version

STATE OF NEW YORK

443--B

2013-2014 Regular Sessions

IN ASSEMBLY

(Prefiled)

January 9, 2013

Introduced by M. of A. DINOWITZ, JAFFEE, STEVENSON, CRESPO, LAVINE, PERRY, COLTON, ARROYO, BOYLAND, ZEBROWSKI, SCARBOROUGH, TITONE, HOOPER, ROSENTHAL, GALEF, KAVANAGH, WEPRIN, ABINANTI, THIELE, CLARK, OTIS -- Multi-Sponsored by -- M. of A. BRENNAN, COOK, GLICK, GOTTFRIED, HIKIND, JACOBS, McDONOUGH, MILLMAN, PEOPLES-STOKES, RABBITT, RAIA -- read once and referred to the Committee on Labor -- reported and referred to the Committee on Codes -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee -- again reported from said committee with amendments, ordered reprinted as amended and recommitted to said committee

AN ACT to amend the labor law and the education law, in relation to prohibiting an employer or educational institution from requesting or requiring that an employee, applicant or student disclose any user name, password, or other means for accessing a personal account or service through specified electronic communications devices

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

Section 1. The labor law is amended by adding a new section 201-g to read as follows:

§ 201-g. Request for access to personal accounts or services prohibited. 1. For purposes of this section, the following words shall have the following meanings:

(a) "Applicant" means an applicant for employment.

(b) "Electronic communications device" means any device that uses electronic signals to create, transmit, and receive information, including, but not limited to computers, telephones, personal digital assistants and other similar devices.

(c) "Employer" means (i) a person or entity engaged in a business, industry, profession, trade or other enterprise in the state; or (ii) a

EXPLANATION--Matter in *italics* (underscored) is new; matter in brackets [-] is old law to be omitted.

LBD03108-05-3

Appendix 9

EDU SOCIAL MEDIA RELATED COURSES
2008-2014

COURSE	SEMESTER/YEAR	DATE
Managing Across Generations in Today's NYPD	Fall 2008	11/21/08
Managing Across Generations in Today's NYPD	Spring 2009	4/30/09
Managing Across Generations in Today's NYPD	Fall 2009	12/7/09
Media Relations	Spring 2010	4/28/10
Managing Across Generations in Today's NYPD	Fall 2010	11/19/10
The Professional Consequences of Social Networking	Fall 2010	12/15/10
The Professional Consequences of Social Networking	Spring 2011	4/15/11
The Professional Consequences of Social Networking	Spring 2011	5/19/11
The Professional Consequences of Social Networking	Spring 2011	6/14/11
Extremist Behavior on The Internet	Fall 2011	10/26/11
The Professional Consequences of Social Networking	Fall 2011	11/10/11
Extremist Behavior on The Internet	Fall 2011	11/26/11
The Professional Consequences of Social Networking	Fall 2011	12/15/11
Smart Devices and Law Enforcement	Spring 2012	1/18/12
Flash/Crime Mobs	Fall 2012	10/17/12
Technology And Law Enforcement	Spring 2013	2/13/13
Flash/Crime Mobs	Spring 2013	2/15/13
Social Media Trends	Spring 2013	4/30/13
Unlocking The Secrets of Social Media	Spring 2013	5/13/13
Smart Devices and Law Enforcement	Spring 2013	5/23/13

Appendix 10

Note: Double Click to open full version

REPORT UNDER
EDU # 07-11

POLICE DEPARTMENT
CITY OF NEW YORK

May 25, 2011

FROM Executive Officer, Executive Development Unit

TO: Police Commissioner (through channels)

SUBJECT: **RECOMMENDATION FOR THE DEVELOPMENT OF AN NYPD SOCIAL NETWORKING POLICY**

1. As part of our training efforts for executives, the Executive Development Unit has conducted extensive research on the impact of Social Media and Networking Sites (SNS) on law enforcement personnel. Since 2008, EDU has been studying the evolvement of this technological innovation, and we have already conducted 3 (three) separate executive seminars in the past year on SNS issues. Our research has uncovered voluminous information on the many ethical and legal perils which SNS usage poses for all law enforcement personnel. Based on all of our efforts, I recommend that the Department establish a broad-based social media policy – and related training – to closely regulate employee use of social media and networking sites. The overall purpose of such a policy would be to protect the reputation of our organization and its employees, as well as to safeguard the NYPD against a host of legal liabilities.

SCOPE

As SNS usage has skyrocketed in recent years, society is fast witnessing the many legal, ethical, and integrity concerns inherent in this new technology. Further, a related trend in the judicial arena indicates that social materials available in the public domain are increasingly being used to undermine and/or impeach witness credibility. In 2009, the New York State Bar Association issued a ruling which states that *"an attorney representing a pending litigation may access the public pages of another party's social materials for the purpose of obtaining possible impeachment material for use in litigation."*[1] This ruling has far-reaching implications for law enforcement professionals; as recent cases attest, attorneys are already using social networking information available on the internet to undermine and/or impeach officer testimony in courtroom proceedings. Given the electronic transparency in today's society, law enforcement agencies nationwide are rapidly seeing the impact of SNS usage. Numerous cases of law enforcement officials posting careless information on their personal sites have already resulted in public relations quagmires for law enforcement agencies[2]. In addition, more defense attorneys and public opinion advocates are realizing that they can now extract – absolutely legally – untold volumes of personal information from the social networking sites of active police officers. As technology usage continues to grow exponentially, the NYPD risks being outpaced by these SNS concerns. The responsibility weighs heavily on the Department to establish guidelines to alert all Department personnel of the hidden dangers of these technologies.

[1] NYS Bar Association, Committee on Professional Ethics, Opinion 843, September 9, 2009.
[2] For one example, see Dean, S. (2010, June 29) *Officer's Racist Postings on Facebook Investigated*. Retrieved from http://www.click2houston.com/print/24083478/detail.html.