Metropolitan Police Academy

1.8 Social Media

1.8.1 Understand departmental regulations governing internet use and social media

Internet Use

Internet use is permitted and encouraged for business purposes in support of the goals and objectives of the Metropolitan Police Department. GO-SPT-302.08 [Metropolitan Police Department Wide-Area Network (MPDNet)] states, in part, that the internet shall be used for official purposes including, but not limited to, the exchange of e-mail about public safety and work-related issues with MPD members, community members, and other police agency partners; performing various forms of work-related research; performing word or phrase searches to locate documents, and the investigation of internet-related crime when so assigned or authorized by a commanding officer or director.

Members shall not use MPD internet access to:

- Pursue private commercial business activities or profit-making ventures.
- Engage in unauthorized fundraising activities of any kind including, but not limited to, the solicitation of funds for personal or financial gain or other non-MPD related benefit.
- Knowingly receive/transmit any files in violation of licensing and/or copyright restrictions.
- Engage in matters directed towards the success or failure of any political party or candidate for office.
- Access any internet sites resulting in additional costs to MPD without advanced authorization.
- Engage in any prohibited discriminatory conduct which could be construed as contributing to a hostile work environment.
- Obtain, view, or send sexually explicit material.
- Engage in activity that violates the privacy of other users.
- Engage in conduct meant to purposely or which could misrepresent the identity of the user.
- Send any material that is obscene or defamatory or which is intended to annoy, harass, or intimidate another person.
- Create a discussion group without written authorization from the MPD-OCTO.
- Post or release MPD data without authorization from the commanding officer or director.
- Transmit sensitive or restricted information.
- Engage in activities that would tend to bring discredit on MPD or that violate laws, regulations, or MPD policy or procedure.

Social Media for Investigative and Intelligence-Gathering Purposes

Executive Order 21-025 provides members with guidance on the use, management, administration, and oversight of social media for investigative and intelligence-gathering purposes. It is important to note that when conducting investigations:

- ***Overt*** monitoring, searching, and collecting of information available in the public domain for any legitimate law enforcement purpose is permitted and requires no supervisory authorization.
- ***Covert***, undercover accounts related to public safety or potential criminal activity may only be used by specific MPD divisions and require prior approval from the Violent Crime Suppression Team (VCSD) commander.

Social Media

What is social media? GO302.03 defines social media as online sources that allow people to communicate, share, and exchange information with others via some form of online or cellular network platform (e.g., Facebook, Twitter, Instagram, LinkedIn). Information may include, but is not limited to, posts, photographs, video, audio, and other multimedia files, message boards, online bulletin boards, and other similarly developed formats, to communicate with others using the same groups while also networking with other users based upon similar interests (e.g., geographical location, skills, occupation, ideology, beliefs).

Social media gives a person almost an unlimited number of avenues to communicate his/her thoughts and share ideas and different types of media such as music, photos, and videos. People also use social media to reconnect with lost friends and share other major moments in their lives with family and friends, some of whom live on the other side of the world. Parents use social media to communicate with or even keep track of their children. However, this method of communication does have its disadvantages. Criminals and terrorists can exploit social media for drug trafficking, child sexual exploitation, and other criminal activity.

Officers need to be aware of the dangers of social media websites and should take precautions to protect their personal information online. Social media is being used more and more to identify officers and their families as well as to report officers' on and off-duty conduct, to include revealing what officers post to their personal social media accounts.

Unless previously released by the department, members shall not post or transmit the following types of information on social network sites:

- Pictures, depictions, descriptions, or personal information of any victim, witness, or suspect.
- Pictures, depictions, or descriptions of any crime scenes.
- Information regarding previous, current, or future investigations.

Members may conduct overt monitoring, searching, and collecting of information available in the public domain with no supervisory permission. If a member wishes to create and use an undercover social media account, he/she must ask for permission through the chain of command to the VCSD Commander.

1.8.2 Identify the risk that personal social media accounts pose to law enforcement officers

Police officers can obtain a lot of information through social media; however, members need to be cautious about what they post online. Police officers from around the country have come under severe scrutiny regarding their posts on their personal social media sites. For example, officers have used social network sites as a place to voice frustrations with work conditions, coworkers, and/or supervisors. Always remember that once you post something online, it may never disappear. When using social media, members must exercise good judgement and refrain from engaging in conduct that undermines their credibility as MPD members. Members shall ensure that their online conduct is consistent with GO 201.26, Duties, Responsibilities, and Conduct of Members of the Department, and this general order, including, but no limited to, refraining from conduct that brings discredit upon themselves, MPD, or the department. MPD recognizes and respects the First Amendment rights of members and community members to participate on social media platforms, but members need to be mindful that their speech becomes part of the worldwide electronic domain. Members shall not use their status as an MPD member to endorse any product or service without prior written permission from the chief of police.

MPD recognizes two general categories of social media use among members.

a. Personal use is the engagement or participation in any personal social media platforms, including but not limited to, personally owned sites, sites of others, news media pages, professional sites unaffiliated with MPD, or other online information exchange forums.
b. Department-authorized use is the engagement or participation in social media platforms for the specific purpose of assisting the department and its members in community outreach, problem solving, crime prevention, and other department-related objectives.

Members seeking to manage personal social media sites that are MPD-focused need to obtain permission from the Office of Communications director, through the member's chain of command, prior to setting up the account. If approved, members shall ensure that the content is posted in compliance with policies and procedures of the department.

Not withstanding any other provision of this order, a member may post to person social media accounts if:

a. He or she expresses a personal viewpoint and does not attribute the viewpoint to the department
b. He or she does not post any information, images, or material that is confidential or privileged

c. He or she does not violate any District of Columbia law

Department-Authorized Use of Social Media

1. Office of Communications staff shall approve public relations social media content. Office of Communications staff members shall maintain the department's official social media presence. Only members authorized by the Office of Communications staff supervisor shall access official department social media platforms. Office of Communications staff shall maintain a list of approved element social media sites.

2. Due to the public's First Amendment free speech rights, comments made by a member of the public shall not be deleted except in cases where the content is derogatory in nature, at the discretion of an Office of Communications supervisor.

3. When establishing an official department social media account, the Office of Communications shall ensure that the account includes the following items:

Department Social Media Account Requirements

a. Statement that clearly specifies that the account is an official MPD platform
b. Statement that indicates that the page is maintained by MPD
c. Disclaimer notice that clearly states the page is not monitored at all times
d. Information on how MPD should be contacted in case of an emergency
e. A link to the MPD website
f. General contact information

4. Members who represent MPD on official department social media accounts shall ensure that all posts contain the appropriate voice, tone, and use of humor, as applicable. Members shall observe all MPD standards of conduct, established social media protocols, proper, decorum and abide by all copyright, trademark, and service mark restrictions when posting to social media.

5. All social media content shall adhere to applicable laws, regulations, and policies. This applies to information technology standards, records retention regulations, content protected by law through copyright, trademark, and service mark restrictions, and public records laws.

6. Members shall not post statements about the guilt or innocence of a suspect or arrestee, comments concerning pending prosecution, and confidential information.

Police agencies around the nation are receiving more and more complaints against their officers regarding what was posted on *personal* social media accounts. The complaint is usually accompanied by a screenshot of what the post includes. In some cases, the screenshot is reposted on another social media accounts and forwarded to a local news agency.

Here are two cases where officers came under fire for comments they posted on their social media accounts:

- In April of 2015, WPTZ aired a story regarding posts on Facebook by a Vermont State Police corporal who appeared to mock Muslims and transgender people on his personal Facebook page. The trooper also mentioned that he wished he could force an electric car driver off the road. The Vermont State Police were made aware of the posts by a Facebook user who filed a complaint against the corporal. The complainant flagged multiple messages. One of the messages stated that Bruce Jenner's transgender identity was evidence of the "Decline of America." The news station interviewed the commander of the Vermont State Police who stated, "This just goes against the fabric of the State Police" and, "This is something that can't be tolerated." You will be shown a video of this incident in class at the academy.

- News Channel 5 in Cleveland aired a story about an East Cleveland police officer who posted comments on Facebook that were called inflammatory during the Ferguson protests. When approached about the comments, the officer stated that his posts were just a joke and taken out of context. His immediate supervisor was interviewed and said that it "wasn't meant for public consumption." You will be shown a video of this incident in class at the academy as well.

Officers need to remember that a news agency has already done its fact-checking and researched you well before a story hits the news. News agencies have employees who are experts in searching social media accounts and use whatever they find that they determine is newsworthy. And they are not going to ask for your permission!

Social media can pose certain risks to law enforcement agencies. Individuals often form groups through social media when they share common beliefs or goals. A hacking group that has received a lot of media attention is ANONYMOUS. Individuals associated with this group have used social media to communicate threats against law enforcement officers. Police departments around the nation have been targeted and have been subjected to cyber-attacks, website defacement, and had sensitive information accessed and released.

In October of 2013, Anonymous posted a video on YouTube addressed to "The Washington D.C. Police Department," warning MPD in advance and threatening that if it unlawfully arrested anyone, they would "unleash hell on our (MPD) servers, phone lines, email, and whatever else they can find." During this event, false information was released on Twitter that there were clashes with police.

Posts like these are designed to spur other individuals to take action against officers either online or during a physical demonstration. These types of posts are also called *Twitter storms*. A Twitter storm is an attempt to post an item on social media for the purpose of generating a significant amount of media attention.

1.8.3 Define crowd sourcing and doxing

Crowdsourcing

Social media poses certain risks not just to law enforcement agencies, but to law enforcement officers and their families. Some individuals and groups have used social media websites as a platform to target law enforcement officers. They are called online actors. Online actors attempt to collect and share information through social media websites. A tactic that is used is known as *crowdsourcing*, a technique that has members of groups/networks use social media to obtain information on a targeted individual or organization, whether legally or illegally.

For example, the National Capital Region Threat Intelligence Consortium (NTIC) published the following incidents:

- During the federal government shutdown in October of 2013, A U.S. Park Police officer based out of the District of Columbia was photographed arresting a participant of the shutdown. A subject affiliated with the Patriots Guild posted on a public Facebook page, "Let's figure out who the Officer is, remove the bollards and shoot him."

- In July 2013, an individual posted on a public Facebook page associated with supporters of a gun-rights activist who had been arrested. In the posts, the individual encouraged the gathering and publishing of the cellular telephone numbers of police officers in the National Capital Region so supporters could flood those officers' telephones with calls.

Members always need to be mindful of potential safety and security issues they may encounter when identifying themselves as law enforcement officers on social media sites. This is also referenced in General Order 302.08. Members are cautioned to be mindful of potential safety and security issues that may occur from:

- Disclosing home addresses, phone numbers, and any other personally identifiable information.
- Posting pictures or depictions of MPD-issued uniforms, to include personally purchased items that reference or resemble any MPD badge, patch, logo, etc.
- Posting pictures of MPD equipment such as vehicles or weapons.

Doxing

How do “online actors” use this information? One method is called *doxing*, a technique where the personally identifiable information of a targeted individual, such as his or her full name, date of birth, address, and/or occupation, is publically released on a social media website without the knowledge or permission of the targeted person. The information is typically obtained from social media websites. Doxing typically leads to a barrage of unwanted phone calls and letters, possible vandalism, and threats to the targeted person.

In April of 2014, the Utah Statewide Information & Analysis Center reported that “Anonymous” had started a renewed effort to obtain and release the personally identifying information of law enforcement officers in an effort called #OpPigRoast. Below is the actual announcement:

> Today we bring you a juicy 0-Day exploit affecting U.S. police forces nationwide. It allows for the simple identification and d0xing of entire police departments. While we have been aware of this exploit since 2002, we have traded it only in private, out of fear of its abuse. The recent actions of the Albuquerque police department, the revelations of Edward Snowden, and the crackdown on the Occupy movement were all events that brought us to release this exploit publicly…We can begin to monitor them. We can call them out. We can make them feel as vulnerable as they try to make us feel. We can turn the tide.

Although this Anonymous action was aimed towards law enforcement officers in Utah, MPD members need to be aware of the lengths this type of group is willing to go to identify and harass law enforcement officers.

1.8.4 Identify methods to protect your personal information on social media

Officers need to be aware of the risks that personal social media accounts pose and how to protect themselves. The best ways to reduce the risk are:

- Reduce or remove your online presence. This alone is one of the best ways to reduce your risk.
- Check your privacy settings on all of the social media sites and apps that you use.
- Be cautious of unknown persons trying to “friend” you.
- Refrain from posting personal information online! Personal information can and is frequently used by online actors.
- Set up multi-factor authentication, something which requires more than one form of authentication (such as a single use code) to verify identity before allowing access.
- Search yourself online and see what information is out there about you.
- Refrain from posting pictures of yourself in uniform or in or by a marked squad car, especially when the picture contains an agency identifier such as a patch or badge.
- Check your credit report regularly and report any errors or inconsistencies.

Summary

Social media integrates user-generated content and user participation. Internet usage is permitted and encouraged for business purposes in supporting the goals and objectives of the department. Members need to be cognizant of what they post online and need to refrain from posting inappropriate and/or unprofessional content on personal social media accounts.

In this lesson, you should have learned MPD's policies governing the use of internet and social media. You should now understand the risk that personal social media accounts play to police officers, such as crowdsourcing and doxing, as well as ways to protect your personal information on social media.