10-217 Social Media Use in Investigations

(xx/xx/xx)
Revisions to prior policies: (12/15/09) (05/24/13) (09/20/21) (09/26/22)

I. Purpose

A. The Minneapolis Police Department (MPD) recognizes that social media can be a useful tool in the investigation of criminal activity, when used in a lawful, non-discriminatory manner. This may include social media actions such as "following" and "engaging with" other accounts to establish a credible covert social media profile, as detailed and authorized in this policy.

B. The purpose of this policy is to provide members with guidance on the use, management, administration, and oversight of social media for investigative and intelligence-gathering purposes. Personal social media accounts are covered by P&P 5-108.

II. Policy

A. Use For Law Enforcement or Public Safety Purposes

1. Social media accounts under this policy shall only be used when ~~they could reasonably aid a legitimate criminal investigation of a person, group or organization, or for intelligence collection efforts related to public safety or potential criminal activity~~. the member has established specific and articulable facts showing reasonable grounds to believe that the data is relevant and material to an ongoing criminal investigation or specific and articulable facts showing reasonable grounds of a safety risk to a large gathering of people (concerts, sporting events, political rallies, public protests, large parties and similar). Personal social media accounts shall not be used for the purposes detailed in this policy.

2. Members shall not use social media accounts to collect and maintain criminal intelligence information about a person or organization unless there is ~~reasonable articulable suspicion (RAS)~~ probable cause that the person is involved in criminal conduct, ~~or activity, and~~ the information is relevant to that criminal conduct ~~or activity~~ and the member has provided good reason to believe leads can be found on social media.

B. Use Department-Approved Equipment

Members shall only use access or use social media accounts under this policy through Department-approved electronic equipment.

C. Approval Requirements for Covert Social Media Accounts

1. Any member seeking to create or use a covert social media account shall obtain prior written approval from the member's Deputy Chief, through the chain of command (supervisor, Lieutenant, etc.) for the account, ~~and~~ the proposed profile details, the members who will access the account, the purpose of the account, and the names/identities of the persons or groups with whom the members will seek to connect. The member shall obtain written approval to continue using the covert account every 60 days.

   If a member needs to create a covert social media account due to an imminent threat or potentially life-threatening situation (such as a hostage situation), they may create the account with Deputy Chief or Watch Commander approval. After the situation is resolved, the member shall notify their chain of command.

   Covert social media accounts shall only be requested when there is no less invasive means available and when a subpoena or warrant to the social media platform is impossible or would not accomplish the law enforcement purpose.

2. These requirements apply to all covert social media accounts, including those used to collect open-source social media information.

D. No Promotion of Violence or Criminal Activity

MPD members shall not post through any social media account any information ~~through a social media account~~ that promotes violence or criminal activity.

NOTE: original phrasing was unclear, it could be read as judging if the social media account promoted violence rather than the post being made by the officer.

E. No Targeting of Constitutionally-Protected Activities

1. Members shall not take any action through any social media account likely to chill the exercise of First Amendment freedoms except where there is reasonable suspicion of criminal activity or planning and clear evidence indicates that the First Amendment–protected activity directly relates to the suspected criminal activity or planning.

2. When social media use during a criminal investigation is reasonably likely to yield information about the exercise of First Amendment–protected rights, data collection should not commence until the following measures have been met:

a. Completion of documentation clearly demonstrating that (i) the expected collection of information about First Amendment rights is unavoidably necessary for the proper conduct of the investigation and (ii) every reasonable precaution has been employed to minimize the collection and retention of information about, or interference with, First Amendment rights.

b. Review by a supervisor confirming specifically that each factor above has been met and approving the social media collection.

F. Subject to MPD and City Policies

1. Social media use in investigations is subject to the requirements of P&P 5-108 Social Media Sites, the City's Electronic Communications Policy and Social Media Policy, and all other applicable MPD and City policies.

2. Members using social media accounts for investigation shall not post, display, or transmit content on their personal social media accounts or through City technology that is disparaging or evidences knowing and intentional discrimination toward a person or group based on protected class status, and that would lead an objectively reasonable person to doubt the member's ability to perform the duties of a peace officer in a fair and impartial manner (P&P 5-104).

3. When using covert social media techniques, conducting investigations, determining likelihood of threat to a public event, or otherwise establishing ~~RAS or~~ probable cause (PC), members shall not consider a person's protected class status, or substitutes for, or stereotypes of race or national origin, to any extent or degree, when taking, or refraining from taking, any law enforcement action, except as provided below:

   Members may consider a person's protected class status only if the demographic descriptors are part of a specific and detailed suspect description tied to a time and place that refers to a person with a particular demographic category and that includes other appropriate non-demographic identifying factors. This consideration must be based on credible and recent information that links specific unlawful or suspicious activity to the person or group, as part of an ongoing criminal investigation. (P&P 5-104)

4. Documentation collected under this policy, including registries and logs, shall be maintained in accordance with the City of Minneapolis' Records Retention Schedules.

5. Documentation collected under this policy is considered investigative data and is subject to MN Stat. 13.82, Subd. 7.

III. Procedures/Regulations

A. Collecting Information from Social Media

Members may collect information available in the public domain for any legitimate law enforcement ~~or public safety purpose~~. This includes monitoring for specific and credible threats and in preparation for significant public sporting, political, or similar events. ~~and s~~ Such activity does not require prior supervisory authorization or activity logging (except the requirements detailed in section [III-E] regarding investigations). This can include the following actions:

- Observing social media accounts and content.
- Searching for social media accounts and content.

NOTE: Public Safety Purposes is an extremely broad and vague category. Tracking the sexual partners of someone with an STD could fall under public safety purposes. The term is not defined in the definitions section.

B. Covert Social Media Profile Creation

If creation of a covert social media account has been approved ([II-C]), the member may create or use the social media account, profile, avatar, or a similar form of online identification.

1. Members shall complete the required training prior to using the account.

2. All profile details shall be fictitious and designed solely to support the authorized investigative objective, including usernames, biographical information, and photos, subject to the following:

   a. Members shall not use the name or other identifying information of any real person without that person's prior consent.

   b. Profile images or avatars shall be created using publicly available stock images or AI-generated images that do not depict real people.

C. Member Responsibility for Account

1. The member registered as the account owner of a social media account is responsible for all content posted online under that profile.

2. The member shall maintain their registered social media account, and shall not share the access information with other members, except that:

a. The member shall provide the password to their registered account upon request from the Commander of the Intelligence Division or their designee, or for auditing purposes.

D. Data Sharing:

a. Data collected should not be shared with other law enforcement agencies absent either a showing of reasonable suspicion that the information contains evidence of criminal activity over which the receiving agency has jurisdiction, or relevance to an ongoing investigation or pending criminal trial in which the receiving agency is engaged. Agencies should have a memorandum of agreement in place confirming that the receiving agency will abide by equivalent limitations in any use or further dissemination of the data.

E. Caution in Interpretation:

a. Members will consider the difficulty in accurately assessing the meanings of posts, pictures, music, videos, and other forms of expression and communication on social media. Individuals use in-group slang, and both law enforcement personnel and algorithmic tools may fail to recognize sarcasm, satire, or hyperbole. Trying to interpret posts by young people, who often use memes and pop culture references that may be inscrutable to outsiders, can intensify these challenges. This effect is likely to be heightened for young people of color and immigrant youths, who are more heavily policed and more susceptible to inaccurate or biased presumptions that gestures, clothing, and other characteristics viewed online indicate gang activity or other criminal behavior.

b. Members who feed pictures drawn from social media into any facial recognition program or use any automated digital surveillance tool or AI/LLM will view any output as leads to be examined in more detail, and not as conclusive evidence.

F. Content Log Requirements

1. Log requirements are limited to original content

a. These logging requirements apply to original content, including but not limited to: original posts, comments made by the member, and direct messages sent.

b. These logging requirements do not apply to social media actions that do not generate ~~original~~ content ~~such as reposts of other user's content,~~ beyond reactions (such as likes), and requests (such as requests to follow).

NOTE: Reposting of another user's content not significantly different from original content should be viewed as if that content was created by the member.

2. Process for logging content

Members using a covert social media account shall maintain a log of all content made through that profile.

a. The log shall include the date and time of the content, the page or profile the content was made on, and the subject of the content.

b. The member shall take screenshots of the content and store them with the log.

c. All content shall be documented in this manner and maintained even if the online content is later deleted.

G. Document Evidence and Demographics of Investigation Subject

Members using a social media account to conduct an investigation shall document in the case file all evidence collected, case numbers or incident numbers related to the investigation, and the following known or perceived demographic categories of every person who is a subject of the investigation:

- Race and ethnicity.
- Age.
- Gender.

H. Oversight

1. Account registration

The Commander of the Intelligence Division shall provide oversight by maintaining a centralized registry of all active covert social media accounts.

a. After accounts are approved per section [II-C], members shall register all covert social media accounts with the Intelligence Division Commander, and shall include the following information:

- The name and web address of the social media site or platform.
- The date the account was created.
- The username and screen name of the social media account.
- The password for the account.
- The employe ID of the member responsible for maintaining the social media account.

i. Members shall notify the Intelligence Division Commander if the information changes (including updating the password).

b. The Intelligence Division Commander or their designee shall conduct yearly audits to confirm whether covert social media accounts are still active.

c. When a covert social media account is no longer needed it shall be deactivated or deleted from the social media site to the extent permitted by the social media site, and the member shall notify the Intelligence Division Commander.

d. In addition to reviewing the data to confirm the active status of accounts, the Intelligence Division Commander or their designee may review accounts to ensure they are being used in compliance with MPD and City policy, and to ensure the supervisory review documentation complies with MPD policy.

2. Supervision

a. Supervisors shall monitor the use of covert social media accounts by their members.

i. Supervisors shall conduct a documented review of all covert social media accounts used by their direct reports on the following timelines:

- Every day a direct message is sent to or received from a minor.
- Every 30 days for accounts with active direct messaging.
- Every 120 days for accounts with no active direct messaging.

ii. In the review, supervisors shall review all content logged and shall ensure that:

aa. Members are operating accounts pursuant to this policy.

ab. Members are not operating accounts in a manner which could be interpreted as biased, unprofessional, or otherwise in violation of policy.

ac. Members are logging content as required.

b. Supervisors may contact the Commander of the Intelligence Division for information on the profiles to facilitate the review.

c. Members shall update their supervisor whenever an account is created or deactivated in accordance with this policy. If a member's unit is assigned a new supervisor or the member transfers units, the member shall provide their new supervisor with a list of their current covert social media accounts.

d. Supervisors shall provide the documentation of their reviews to the Intelligence Division Commander for storage with the registry.

Definitions

Covert Social Media Account: Account maintained by an MPD member, on behalf of MPD, but in a username not associated with the MPD member, for the purposes of furthering criminal investigations, gathering evidence for criminal investigations, or intelligence collection efforts related to public safety.

Social Media Actions:

Follow: Subscribing to a feed of an account's activity.

Message: A direct or private communication sent between specific users. This includes direct messages, chats, etc. Unlike public posts or comments, messages are only visible to the sender and the recipients.

Post: Uploading content to a page or profile, or adding an original comment to content uploaded by another user. This includes comments, replies, posts (including uploading material someone else created), images, videos, etc.

React: Using a built-in function to indicate appreciation or another emotional reaction to another account's content. This includes using a "Like" button or other preset option that does not add a text comment.

Repost: Sharing another account's content. This includes functions such as retweet, share, repin, etc.

Request to Connect: A request sent from one account to another account to establish a mutual sharing relationship, requiring the recipient to confirm or accept the request to provide access to content not available to other accounts. This includes functions such as Facebook's "Friend" requests.

Request to Follow: A request to subscribe to a feed of an account's activity that requires the account to approve the request. This includes functions such as a Follower Request in "X" (formerly Twitter).

REFERENCE

Principles for Social Media Use by Law Enforcement | Brennan Center for Justice Brennan Center for Justice: NYU Law. R.L. Waldman. Feb 7, 2024