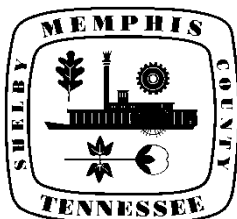


EXHIBIT A



MEMPHIS POLICE DEPARTMENT

Policy and Procedure



SERIAL:

DATE:

FROM:

TO:

SUBJECT: LAW ENFORCEMENT UTILIZATION OF SOCIAL MEDIA

PURPOSE:

To establish guidelines for the use of social media, via manual social media searches and through the use of social media collators, for all MPD Employees as well as all civilians assigned to the Office of Homeland Security (“OHS”) and Real Time Crime Center (“RTCC”), and in compliance with the Order, Judgment, and Decree entered in Civil Case 76-449 (“*Kendrick* Consent Decree”), and in accordance with the Memorandum Opinion issued by the United States District Court in Case No. 2:17-cv-02120, Doc. 151.

SCOPE:

This policy applies to all MPD Employees who utilize social media in the course of their duties, as well as to all MPD personnel with access to social media collators.

GENERAL:

Social media is a tool for real time communication and has become an integral part of daily life for citizens of all ages. Its usage can be a valuable tool to aid in investigations and analysis within public safety interest areas. Similarly, in the aftermath of a crime, social media can be used to obtain information to identify suspects, victims and witnesses.

Social media, by definition, is a forum on which the expression of First Amendment rights may be expected to occur. The MPD’s use of social media is governed by the *Kendrick* Consent Decree.

This policy shall outline the restrictions and uses of social media by applicable officers. This policy is intended to address social media in general, and not any one particular form of social media.

DEFINITIONS:

Assessment – Assessments may be carried out to detect, obtain information about, or prevent or protect against crimes or threats to public safety. Assessments may be undertaken proactively with such objectives as detecting criminal activities; obtaining information on individuals, groups, or organizations of possible investigative interest, either because they may be involved in criminal or public safety-threatening activities or because they may be targeted for attack or victimization by such activities. Assessments require an authorized purpose but not any particular factual predication.

Command Staff - The MPD Command staff includes the Director of Police, Deputy Director, and the six Deputy Chiefs.

Criminal Investigation - If probable cause exists that a crime has been committed, a criminal investigation is the process of collecting information or evidence about an incident in order to: (1) determine if a crime has been committed; (2) identify a perpetrator; (3) establish probable cause; (4) apprehend the perpetrator; and (5) provide evidence to support a conviction in court.

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

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

Political Intelligence – the gathering, indexing, filing, maintenance, storage or dissemination of information, or any other investigative activity, relating to any person’s beliefs, opinions, associations or other exercise of First Amendment rights. Political intelligence includes any investigation into the lawful exercise of First Amendment rights, even if the investigating officer does not have a partisan political motive. Political intelligence is not

permissible as a goal of an investigation nor as the means to an end of an otherwise lawful investigation.

Preassessment – During a preassessment investigation, an officer may gather information using various forms of publicly available online information and paid-for-services databases. No authorization is required for preassessment information-gathering.

Predicated Investigations - The purposes or objectives of predicated investigations are essentially the same as those of assessments, but predication as provided in these is needed - generally, allegations, reports, facts or circumstances indicative of possible criminal or public safety-threatening activity. Supervisory approval must be obtained to initiate predicated investigations.

Public Assembly -- A Public Assembly is any meeting, march, demonstration, picket line, rally, or gathering of more than 25 persons for a common purpose as a result of prior planning that interferes with or has a tendency to interfere with the normal flow or regulation of pedestrian or vehicular traffic or occupies any public area in a place open to the general public, to the hindrance of others.

Public Domain — Any Internet resource that is open and available to anyone, without use of a password, specific invitation, or other identifier.

Social Media — A category of Internet-based resources that integrate user-generated content and user participation.

Social Media Collator — A tool used to capture data and monitor social media sites by utilizing automated tools such as web crawlers and word search functions to make predictive analysis, develop trends, or collect information.

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

Special Events — "Special Events" include parades, races or any other event not meeting the definition of a public assembly.

Spontaneous Events -- Events occasioned by news or affairs coming into public knowledge within seven days of a public assembly.

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

USE OF SOCIAL MEDIA GENERALLY

The collection and use of information through the use of social media shall be conducted in accordance with the *Kendrick* Consent Decree, and the Memorandum Opinion issued by the United States District Court in Case No. 2:17-cv-02120, Doc. 151, which may be found on the Memphis Police Department Kiosk [show link here], and shall further be conducted without violating constitutionally protected rights, or the requirements of 28 CFR Part 23¹, or any relevant state or local regulations.

Social media shall not be used by MPD to conduct political intelligence. Political intelligence, as defined by the *Kendrick* Consent Decree, is the gathering, indexing, filing, maintenance, storage or dissemination of information, or any other investigative activity, relating to any person’s beliefs, opinions, associations or other exercise of First Amendment rights. Political intelligence includes any investigation into the lawful exercise of First Amendment rights, even if the investigating officer does not have a partisan political motive. Political intelligence is not permissible as a goal of an investigation nor as the means to an end of an otherwise lawful investigation. (See DR 138.)

All searches of social media by an MPD employee, including but not limited to those through the use of a social media collator, shall be based on a legitimate law enforcement purpose, and not for the purpose of gathering information related to First Amendment rights. Absent authorization to conduct an investigation, for example, impermissible search terms might include a phrase or name of an organization that expresses political beliefs, such as "Black Lives Matter," "Occupy Wall Street" or "Sovereign Citizens." An example of permissible search terms, which in and of themselves indicate unlawful conduct not protected by the First Amendment, would be “shoot the police.” However, the use, retention, or dissemination of information collected by searches that relate to the exercise of First Amendment rights is governed by the Consent Decree. A search term such

¹ 28 CFR Part 23 is a federal regulation that provides guidance to law enforcement agencies on the implementation standards for operating multijurisdictional criminal intelligence systems funded under the Omnibus Crime Control and Safe Streets Act of 1968, as amended (Crime Control Act)

as “St. Jude Marathon” is permissible because it does not involve the collection of information associated with a person’s exercise of First Amendment rights.

Social media may not be used to seek or retain information about an individual’s age, race, ethnicity, citizenship, place of origin, disability, gender, or sexual orientation, unless for a legitimate law enforcement purpose or if required for identification. Social media may also be used to determine if a person is a minor.

In the event a MPD Employee encounters information on social media pertaining to an imminent threat to public safety or evidence of the planning or commission of a crime, the MPD Employee shall immediately notify his/her commanding officer.

Only social media content directly relevant to the criminal investigation should be retained and disseminated, and it shall be placed in the case file.

Use of social media while on duty should be conducted for police business purposes only, and only in compliance with this Policy. The officer’s personal use of the social media platform and any searches conducted for personal reasons are nevertheless subject to this reporting requirement, when:

- The information searched, gathered, collected, stored or disseminated involves, includes, intersects or overlaps with, or otherwise relates to or has direct or derivative use in any investigation, inquiry or matter involving official law enforcement or department interest; and
- The officer has knowledge of such investigation, inquiry, or matter, or should reasonably have such knowledge.

USE OF SOCIAL MEDIA FOR INVESTIGATIONS UNRELATED TO THE EXERCISE OF FIRST AMENDMENT RIGHTS

For purposes of investigations, MPD employees may use different methods of online investigation based on the phase of investigation: the pre-assessment phase, assessments, and predicated investigations.

- **Pre-assessment phase:** An MPD employee may search and review various forms of online information, including various government systems and paid-for-services databases, as well as information available to the public via the Internet. The use of fictitious information to register for access is prohibited, however. Information obtained in a public chat room may fall within the category of “publicly available information.” An MPD officer may use his or her official email for the limited use of conducting a “clarifying interview” and must identify him- or herself as being affiliated with MPD.

No prior authorization is required for a pre-assessment level investigation.

- **Assessments:** Assessments require an authorized purpose but not any particular factual predication. In an assessment, an MPD officer may use all investigative methods authorized prior to the opening of an assessment, and may also use automated regular searches (*e.g.*, Google alerts) to conduct regular searches of publicly available information. During an assessment, an MPD employee can also access private or restricted-access online forums if an exception to the search warrant requirement has been satisfied, such as through consent by a party with the authorization to access and control content on the site. This “consenting party” may be the account-holder for a social networking site, a system administrator, or a company official with authority to direct others regarding site content. An MPD employee may also record or monitor online public, real-time communications, but not private, real-time communications, which are available only during predicated cases. In addition, an MPD employee should generally deal openly with the public during an assessment. That is, in general, an MPD employee cannot engage in undercover activity in an assessment because it is too invasive. He or she can, however, task sources to access a restricted website to gather information, if the source has authorized access, *e.g.*, consent.
- **Predicated Investigations:** The purposes or objectives of predicated investigations are essentially the same as those of assessments, but predication is needed. Predication can be based on allegations, reports, facts, or circumstances indicative of possible

criminal or public safety-threatening activity. Supervisory approval must be obtained, to initiate predicated investigations. Corresponding to the stronger predication and approval requirements, all lawful methods may be used in predicated investigations including all online investigative methods authorized prior to the opening of an assessment or during an assessment are authorized, as well as additional online methods such as (1) monitoring private, real-time online communications; (2) intercepting communications of a computer trespasser; and (3) undercover activity.

MPD employees shall adhere to MPD's Standard Operating Procedures for opening a predicated investigation.

ONLINE INVESTIGATIONS THAT MAY RELATE TO THE EXERCISE OF FIRST AMENDMENT RIGHTS

MPD employees may only collect information relating to the exercise of a First Amendment rights if (1) the collection is logically related to an authorized investigative purpose, (2) the collection does not materially interfere with the ability of an individual or a group to engage in the exercise of constitutionally protected rights, and (3) the method of collection is the least intrusive alternative that is reasonable, based upon the circumstances of the investigation.

If an assessment or investigation involves the monitoring or interception of communications of a person or group exercising First Amendment rights, that investigation must be authorized pursuant to Section G of the Consent Decree. In those instances, an Authorization Form must be completed and signed by the Director or his or her designee before the more intrusive online investigation methods may be used to gather information about the person or persons exercising their First Amendment rights online.

In no event may MPD base its investigatory conduct solely on an individual's or group's exercise of First Amendment rights.

ONLINE MONITORING OF JUVENILES ON SOCIAL MEDIA

Any and all restrictions regarding the monitoring of juveniles included in MPD's practices, policies, or procedures, are incorporated into this Social Media Policy.

MPD officers may use a social media account, including a covert account, to contact or connect with a minor, without first notifying that minor's parent or guardian, only as allowed by Tennessee law and as authorized by § G of the consent decree.

DOCUMENTATION AND RETENTION

Other than crime analysis, situational assessment reports, and evidence collected during a criminal investigation, no information obtained from social media websites shall be retained.

Information gathered from a social media site by MPD related to First Amendment activity shall not be retained, unless for a legitimate law enforcement purpose, for more than fourteen days.

All social media search terms used by an MPD Employee shall be retained until reported to the Command Staff, which shall occur approximately every 90 days. At the end of each 90-day period, each MPD Employee who conducted a search on social media must submit a list of search terms used to search the particular social media platform related to the officer's duties and responsibilities as an officer of the MPD. These reports shall be submitted to the officer's commander.

Unannounced internal audits of an officer's social media searches are permissible at any time for any reason when authorized by a member of the Command staff.

Situational awareness reports² may be prepared for special events, public assemblies, and spontaneous events management, including First Amendment-protected activities, where necessary for the furtherance of public safety. Employees preparing such reports must take special care to collect no more information than necessary regarding the exercise of First

² A situational awareness report is report of intelligence gathered by law enforcement related to public safety surrounding a planned gathering of people in public. The purpose of a situational awareness report is to provide MPD with information so that it can adequately prepare for and protect the public before, during, and after a special event.

Amendment-protected rights. Employees should further document that there is a relationship between the incidental collection of information about First Amendment-protected activities and the purpose of the report, which is the protection of public safety. At the conclusion of the situation or First Amendment-protected event, the information obtained from social media or from a social media monitoring tool will be retained for no more than fourteen days. At the conclusion of the situation or First Amendment-protected event that was the catalyst for generation of a situational awareness report, and where there was no criminal activity related to the information gathered, the information obtained from social media or from a social media monitoring tool will be retained for no more than fourteen (14) days, or, if needed to create an After Action Review, up to ninety (90) days.

After Action Reviews may be prepared using information gathered from social media. "After Action Review" (AAR) is defined as a report following an incident describing the incident and analyzing MPD's preparation for and response to reaction to the incident. The information obtained from social media may be retained within the AAR indefinitely, but the names, photos, and identifying information of individuals and organizations not suspected of criminal activity should be redacted.

Information from social media that does indicate a criminal nexus of unlawful conduct that is not protected by the First Amendment may be retained in an intelligence report, suspicious activity report, or case investigative file.

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

At no time shall MPD Personnel maintain any social media files outside of these authorized files.

DISSEMINATION

Information gathered from social media, including screen shots or “snags” of social media sites, shall not be disseminated except as necessary for preparations for special events, spontaneous events, and public assemblies management or for the investigation of unlawful activity. Information gathered from social media may not be forwarded or shared beyond those who are authorized by this Policy. Any information gathered and retained from social media may only be disseminated to MPD Employees and staff as necessary.

DISCIPLINE

Any employee who violates this Section will be subject to disciplinary action, up to and including termination.

Cross Reference

DR 138