

Model Policy for Law Enforcement Investigative use of Social Networking

Disclaimer: This is a model policy was designed to provide a guide to writing a policy related to social networking use. This model policy should be reviewed and revised based on your local legal requirements. Implementation of any of this model policy should be done so only after legal review by your agency attorney. Additionally, your policy prior to implementation will need to conform to any national or local laws, labor agreements and existing policy within the agency.

I. POLICY

That all <Agency Name> police department personnel use computers, computer applications, computer programs, Internet resources and network/Internet communications in a responsible, professional, ethical, and lawful manner. That conduct of its employees off off-duty has a reflection on the department. This policy is intended to guide employees conduct when it relates to their employment or representations of employment though the numerous social networking venues. The <Agency Name> police department has established guidelines for conducting surveillance, undercover, decoy, and raid operations. Investigations using Social Networking are specialized investigative operations requiring an understanding of the new technology and its impact on the community. These investigations can be very effective in determining criminal activities of individuals or groups both online and in our community. At times, social networking investigations may provide the only technique available to identify principals and co-conspirators involved in criminal activity. Social Networking investigations may be conducted against any type of crime including: organized crime, narcotics, burglars, vice suspects, stalking, child predators and other individuals or groups who commit criminal acts.

II. POLICY REVIEW

This policy will be reviewed by the <Appropriate administrative level Supervisor> or any person so designated by the <Chief of Police, Sheriff or lead Law Enforcement Administrator> on an annual basis to ensure that it is legally sound and reasonably enforceable.

III. POLICY TRAINING

All full-time officers, administrative staff, support personnel, student interns, volunteer staff and/or any other persons so authorized to use the police department computers will become familiar with and adhere to the provisions of this policy and receive training and notification pertaining to this policy by in-service training, internal mail, email, and/or occasional network log-on reminders

IV. DEFINITION OF “SOCIAL NETWORKING”

Is defined as social network sites that use Internet services to allow individuals to construct a public or semi-public profile within that system, define a list of other users with whom they share some connection, and view and access their list of connections and those made by others within that system. The type of network and its design vary from site to site. Examples of the types of Internet based social networking sites include: blogs, networking sites, photo sharing, video sharing, microblogging, podcasts, as well as comments posted on the sites. *The absence of, or lack of explicit reference to a specific site does not limit the extent of the application of this policy.*

V. SOCIAL NETWORKING INVESTIGATIVE OPERATIONS:

Social Networking investigations have no different requirements when it comes to documenting the investigations. The techniques applied on the Internet still require the information be properly collected, properly preserved and properly presented in a report.

The objective of social networking investigations is to:

1. Determine the nature of the online criminal activity.
2. Identify all of the persons involved in the online criminal activity.
3. Legally obtain evidence for a search warrant or for prosecution.
4. Obtain evidence of the crime from social networking sites.
5. Verify investigators online actions.
6. Prevent the commission of further crime and apprehend subjects committing crimes through social networking sites.
7. Develop leads based on information from other sources.

VI. PROFESSIONAL CONDUCT ONLINE

Officers realize their obligation to the community and should strive to act in a professional manner while investigating crimes on the Internet in order to inspire the public trust and confidence. Maintaining professionalism, even while online, should be a primary goal our officers and will ensure the continued trust and respect of the community. All officers are public servants and shall keep all contacts with the public both professional and courteous.

VII. PREPARING FOR A SOCIAL NETWORKING INVESTIGATIVE OPERATION:

Prior to determining if a social networking investigative operation is necessary or useful, the designated supervisor or investigator in charge will conduct an analysis of all available information, which may include victim information, review of F.I. cards from the area, criminal intelligence data, confidential informant information, and information from police officers or police reports from the neighborhood or target area where officers will work.

The supervisor or investigator in charge of the specialized investigative operation will:

1. Closely supervise the operation.
 - a. including any large scale undercover operation.
2. A Supervisor with the rank of Sergeant or above has the authority to conduct a small scale operation which encompasses his or her squad with the approval of the Divisional Commander.
3. Supply or have access to the computer equipment required for the investigation. The

- equipment may include:
- a. Online Investigations computer
 - b. Investigative Internet access (not tied to the agency)
 - c. Online evidence collection software
 - d. Any other equipment the supervisor determines to be necessary.
4. Determine operational procedures and guidelines for arrest, if applicable, including:
 - a. Where the operation will start from.
 - b. What is expected of each officer.
 - c. When and where the arrest will take place.
 - d. Any other information which is necessary to successfully complete the operation.
 5. Obtain and authorize undercover identities.
 6. Obtain false credentials when necessary.
 7. Determine what funds need to be made available and provide funds as required to the undercover personnel. Requests for investigative funds will be handled as described by agency directive.
 8. Determine what legal problems may be encountered and what action is necessary to resolve them.
 9. The supervisor may require the investigator in charge of a large scale social networking investigations to complete a plan of the operation, which is not part of the case file, containing what is currently known about the suspect(s) and target areas. This may be accomplished through an analysis of the available information and should include, but is not limited to, the:
 - a. Suspect(s) activities, habits, vices, occupation, hobbies, and crimes.
 - b. Suspect(s) work and residential address, including the neighborhood environment using maps, aerialphotos, and/or driving in the area, if possible.
 - c. Known vehicle(s).
 - d. Family, associates and friends.
 - e. Review of F.I. cards of persons who have had contact with the police.
 - f. The plan of operation and all applicable information will be provided to all members participating in a large scale social networking investigation. Information of a sensitive nature may be withheld or distributed in a limited manner at the discretion of the supervisor or investigator in charge, as long as it does not compromise the safety of any involved member.
 10. Assure the investigator is properly prepared for the assignment.
 - a. The officer best suited for each particular operation will be selected.
 - b. The officer will adapt review and understand the persona he has adopted online.

VIII. INVESTIGATIVE REPORTS

The assigned supervisor must review and approve all investigative reports and material, which are prepared and submitted by the investigative officer. Once approved, all investigative reports and material will become a part of a numbered investigative file. Officers must include all relevant information in their investigative reports concerning:

- a. Criminal activity
- b. Suspect identification and disposition
- c. Contraband information and identification
- d. All monies expended for evidence.
- e. Description and disposition of all property seized for forfeiture.

IX. UNDERCOVER SOCIAL NETWORKING INVESTIGATIONS

1) General Authority And Purpose

<Agency Name> police department may engage in undercover activities and undercover operations pursuant to these Guidelines that are appropriate to carry out its law enforcement responsibilities, including the conduct of preliminary inquiries, general crimes investigations, and criminal intelligence investigations. In preliminary inquiries, these methods may be used to further the objective of inquiry into possible criminal activities by individuals or groups who use social networking to determine whether a full investigation is warranted. In general crimes investigations, these methods may be used to further the investigative objectives of preventing, solving, and prosecuting crimes. In criminal intelligence investigations – i.e., racketeering enterprise investigations and terrorism enterprise investigations – these methods may be used to further the investigative objective of ascertaining such matters as the membership, finances, geographical dimensions, past and future activities, and goals of the enterprise under investigation, with a view to the longer range objectives of detection, prevention, and prosecution of the criminal activities of the enterprise. These guidelines do not apply to investigations utilizing confidential informants, cooperating witnesses or cooperating subjects, unless the investigation also utilizes an undercover employee.

Undercover operations will only be used by the law enforcement agencies where they judge such use to be proportionate to the seriousness of the offence(s) being investigated and the history and character of the individual(s) concerned. Online undercover operations should not be used as a speculative means of search for the existence of a criminal offense, where no other grounds exist to suspect that criminal offenses have been or are being committed

2) DEFINITIONS

- A. “Undercover Activities”** means any investigative activity involving the use of an assumed name or cover identity by an employee of the agency or another Federal, state, or local law enforcement organization working with the agency.
- B. “Undercover Operation”** means an investigation involving a series of related undercover activities over a period of time by an undercover employee, whether on the Internet or not. For purposes of these Guidelines, a “series of related undercover activities” generally consists of more than three separate substantive contacts by an undercover employee with the individual(s) under investigation. However, undercover activity involving sensitive or fiscal circumstances constitutes an undercover operation regardless of the number of contacts involved. A contact is “substantive” if it is a communication with another person, whether by oral, written, wire, or electronic means, which includes information of investigative interest. Mere incidental contact, e.g., a conversation that establishes an agreed time and location for another meeting, is not a substantive contact within the meaning of these Guidelines.

NOTE: In the context of online communications, such as e-mail and Internet Relay Chat (IRC), multiple transmissions or e-mail messages can constitute one contact; much like a series of verbal exchanges can comprise a single conversation. Factors to be considered in determining whether multiple online transmissions constitute a single contact or multiple contacts include the time between transmissions, the number of transmissions, the number of interruptions, topical transitions, and the media by which the communications are exchanged (i.e., e-mail versus IRC).

- C. “Undercover Employee”** means any employee of the agency, or employee of a Federal, state, or local law enforcement agency working under the direction and control of the agency in a particular investigation, whose relationship with the agency is concealed from third parties in the course of an investigative operation by the maintenance of a cover or alias identity.

3) Types of Online Undercover Operations

Online Undercover Operations are the use of a pretext to gain the confidence of persons involved in criminal activities on the Internet. It implies anyone engaged in this type of activity must have the ability to establish a relationship with the suspect online in order to determine the nature of his or her activities. An Online undercover operation may encompass several types of assignments which may include, but are not limited to:

- A. Single Operation Assignment:** an online undercover operation on a gambling site, a prostitution website or posting on a bulletin board, illegal pharmaceutical drug sales, or a person who deals in stolen property.

- B. Multiple Operation Assignment:** an investigation of crimes encompassing several websites and or physical locations such as gambling operations or bookmaking, parimutual betting operations, prostitution activity, or a sales of stolen property from a theft ring.
- C. Long-Range Penetration Assignment:** an operation directed toward the upper-echelon leaders of an illegal activity.
- D. Intelligence Gathering Assignment:** a type of online undercover operation which is not directed toward any specific type of illegal activity. The operation may be used as a listening post for general information in a general geographic location where illegal activities are believed to be occurring. Any collection of intelligence on specific persons or groups that fall within the guidelines as identified in 28 C.F.R. PART 23 need to comply with the Federal rules.

4) Online Undercover Operational Plans

Operational plans for the conduct of undercover operations on social networking are intended to guide officers through the execution of an enforcement action. They provide for the assignment of personnel, identification of suspects, equipment and locations (both physical and online) and play a significant role in the safety of officers involved.

- A.** An operational plan will be prepared for each significant social networking investigation or enforcement operation.
- B.** The operational plan will be generated on an established format and shall note the case and any deconfliction procedures taken. The operational plan will state a clear objective and detail the specific roles and assignments of each participating officer. A follow on plan should be completed when the operation moves to a physical arrest situation or a search warrant execution.
- C.** The operational plan will be reviewed by a supervisor or his designee prior to the execution of the enforcement action and maintained in the case file.

5) Deconfliction

Online undercover investigations have the very real potential for multiple agencies to be conducting similar investigations on the same criminal suspects, website, social networking sites or organizations at any given time. There are serious safety considerations in such situations that may bring law enforcement Investigators into high-risk situations without realizing the presence of other law enforcement Investigators. Similarly, such parallel investigations, conducted independently, are less efficient and effective than cooperative law enforcement efforts conducted in a coordinated manner.

- A. All officers should attempt to utilize deconfliction, where practicable. Where formal deconfliction agreements with other agencies do not exist the officer, or his supervisor, should notify the appropriate law enforcement agencies within the area of operation, if identified through the investigation, to ensure appropriate deconfliction has been conducted.
- B. On any investigative activity conducted by an officer outside his assigned area of responsibility, the supervisor shall notify the affected law enforcement agencies, either local or federal, of the desired investigative efforts within their area. This notification should occur prior to beginning the investigative activity or as soon as it becomes apparent that the online investigation has an identified suspect not in the local jurisdiction. It shall be the responsibility of the supervisor to ensure proper deconfliction is conducted.
- C. Any investigative activity that takes an officer physically out of his assigned area of responsibility will require prior notification of the appropriate law enforcement agencies within the area of operation.

6) Conducting Online Undercover Operations

Covert undercover operations on the Internet and Social Networking are an effective investigative technique in establishing admissible, credible evidence in support of a criminal prosecution against suspects. The ultimate goal of any online undercover operation is a criminal conviction. To that end, every aspect of undercover operations should be well planned, deliberate and performed in compliance with all applicable policies. The actions of undercover officers on the Internet should always be appropriate, under the circumstances, and easily justified to prosecutors, judges and juries. Officers conducting covert Internet and social networking investigations to obtain evidence for criminal prosecution will conduct such investigations under the following guidelines:

- A. Officers will obtain the approval of a supervisor prior to the initiation of an undercover involving social networking sites investigation.
- B. Officers will corroborate undercover investigations with the assistance of other officers conducting surveillance of the case officer, informants and suspect(s).
- C. When possible, officers will utilize investigative computer systems and software intended to record data from the Internet and audio and/or video recording in an evidentiary manner when contacting suspects. All video or audio recordings made from the social networking site being used in the investigation shall be considered as evidence and handled as such, regardless of the quality of the recording. All video and audio recordings will be maintained as evidence until the case receives a final disposition.

- D. Officers will not transfer or make available for download any files that they knowingly contain any malicious code or other type of file that would disrupt, delay, or destroy another person's computer system,
- E. Officers will follow all local guidelines and Federal law when conducting undercover operation on social networking sites.
- F. **Terms of Service** Social networking sites require that users, when they sign up, agree to abide by a terms of service (TOS) document. Agency employees are responsible for reading and understanding the TOS of the sites they use during an undercover investigation. TOS agreements may ban users who give false names or other false information during the registration process which may affect the investigation if the use of an undercover identity is discovered by the social networking site.

6. Participation in Otherwise Illegal Activity by Undercover Employees

Except when authorized pursuant to the agency's general Under Cover operation Guidelines, no undercover employee on the Internet shall engage in any activity that would constitute a violation of Federal, state, or local law if engaged in by a private person acting without authorization. For purposes of these Guidelines, such activity is referred to as otherwise illegal activity.

7. Review of Conduct

From time to time, during the course of the undercover operation, the Chief of Investigations shall review the conduct of the undercover employee(s) and others participating in the undercover operation, including any proposed or reasonably foreseeable conduct for the remainder of the investigation. Any findings of impermissible conduct shall be discussed with the individual and promptly reported to the designated Supervisor for a determination to be made as to whether the individual should continue his or her participation in the investigation. Any unacceptable conduct discovered in violation of this or other departmental policy shall be forwarded for review by the agency Internal Affairs Division.

8. Protecting Innocent Parties Against Entrapment

Entrapment must be scrupulously avoided. Entrapment occurs when the Government implants in the mind of a person who is not otherwise disposed to commit the offense the disposition to commit the offense and then induces the commission of that offense in order to prosecute.

9. Identifying and Managing Employee Stress

Investigative personnel encounter a range of assignment-specific challenges and strains based on their participation in undercover operations and contact with material that over time can be emotionally detrimental. The cumulative effects of these strains, together with repeated

exposure to disturbing images and situations, may result in stress reactions that require the attention of agency managers. Supervisors managing employees working in an undercover capacity on the Internet will monthly evaluate the employee's ability to continue in that capacity. Referrals to agency approved Employee Assistance Program (EAP) at a minimum may be appropriate. Reassignment of employees to a less stressful position may be warranted based on the supervisor's evaluation of the employees needs.

Model Policy