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:

MEMBER OF THE SERVICE

1. Confer with supervisor, if access to public domain data requires the use of an online alias/online alias access.
   a. No conferral or authorization is required for general research, topical information or other general uses that do not require the acquisition of an online alias/online alias access.

IF APPLICATION FOR ONLINE ALIAS DOES NOT INVOLVE SUSPECTED TERRORIST ACTIVITY:

SUPERVISOR

2. Evaluate request to determine whether an online alias would serve an investigative purpose, and if so, prepare **Typed Letterhead** requesting an online alias to bureau chief/deputy commissioner concerned.
3. Include on **Typed Letterhead**:
   a. Purpose for the request (i.e., type of investigation, etc.)
   b. Tax registry number of requesting member
   c. Username (online alias)
   d. Identifiers and pedigree to be utilized for the online alias, such as email address, username and date of birth.
      (1) Do not include password(s) for online alias and ensure password(s) are secured at all times.
   e. Indicate whether there is a need to requisition a Department laptop with aircard.
4. Review photograph to be used in conjunction with online alias, if applicable.
   a. Consider the purpose for which the photograph is being used and the source of the photograph.
   b. Attach a copy of the approved photograph and indicate on **Typed Letterhead** how photograph was obtained.
5. Forward request to commanding officer for review.

COMMANDING OFFICER

6. Review request(s) and consider the purpose and whether granting approval would serve an investigative purpose.
7. Endorse request(s) indicating APPROVAL/DISAPPROVAL within one day of original request and if APPROVED, immediately forward approval to bureau chief/deputy commissioner concerned, through channels, for informational purposes.
8. File copies of requests in command.

MEMBER OF THE SERVICE

9. Maintain record of online alias in case records management systems or appropriate Department records.

BUREAU CHIEF/DEPUTY COMMISSIONER

10. Maintain folder for each APPROVED online alias.
    a. Designate an administrator for the online alias.

IF APPLICATION FOR ONLINE ALIAS INVOLVES SUSPECTED TERRORIST ACTIVITY:

SUPERVISOR

11. Immediately contact Intelligence Division, Operations Desk supervisor and provide details regarding proposed investigation.

INTELLIGENCE DIVISION, OPERATIONS DESK SUPERVISOR

12. Determine if investigation should be conducted by the Intelligence Division and proceed accordingly.
13. Notify requesting supervisor to proceed with investigation if it has been determined that the investigation will not be conducted by the Intelligence Division.

SUPERVISOR

14. Comply with steps "2" through "10", as appropriate, if investigation will not be conducted by the Intelligence Division.

WHEN EXIGENT CIRCUMSTANCES EXIST THAT WOULD WARRANT THE IMMEDIATE USE OF AN ONLINE ALIAS:

SUPERVISOR

15. Confer with Intelligence Division, Operations Desk supervisor, if there is concern that the investigation may involve suspected terrorist activity.
    a. Comply with instructions from Intelligence Division, Operations Desk supervisor.
16. Confer with commanding officer/executive officer, if investigation does not involve suspected terrorist activity.
17. Instruct member of the service to proceed with investigation upon receiving APPROVAL from commanding officer/executive officer.
    a. Comply with steps "2" through "10", as appropriate, and include in **Typed Letterhead**, the circumstances that led to the determination of exigent circumstances.

ADDITIONAL DATA

LEGAL CONSIDERATIONS

During the course of an investigation, a member of service may need access to information regarding online accounts maintained by service providers. The federal Electronic Communications Privacy Act (ECPA) governs seizures of electronic evidence. Some information may be obtained with a subpoena; other information requires a special court order; and still other information requires a search warrant. Pertinent sections of the ECPA are as follows:

a. A subpoena is generally deemed sufficient to obtain information such as user information and payment records.

b. Electronic communications, such as email content, in electronic storage for 180 days or less may be obtained only after the issuance of a search warrant, and delayed notification to the subscriber or customer may be ordered if specifically requested in the search warrant application.

c. Electronic communications in electronic storage for more than 180 days may be obtained with a subpoena signed by a judge; however, notice must be provided to the subscriber or customer unless the electronic communications are obtained after the issuance of a search warrant allowing for delayed notification.

ADDITIONAL DATA (continued)

d. *In anticipation of the issuance of a search warrant, a member of the service may send a request known as a "preservation letter" to an electronic service provider requesting the preservation of electronic records for 90 days, and extend the request for an additional 90 day period.*

Note that particular service providers are known to ignore non-disclosure orders (i.e., some service providers will disclose the existence of a search warrant or subpoenas to a subject subscriber or customer.) In general, members of the service should consult with the Legal Bureau before seeking electronic communication through a search warrant or otherwise.

Data obtained through a grand jury subpoena or court order cannot be shared with other law enforcement agencies unless otherwise authorized.

OPERATIONAL CONSIDERATIONS

When a member of the service accesses any social media site using a Department network connection, there is a risk that the Department can be identified as the user of the social media. Given this possibility of identification during an investigation, members of the service should be aware that Department issued laptops with aircards have been configured to avoid detection and are available from the Management Information Systems Division (MISD). A confidential Internet connection (e.g., Department laptop with aircard) will aid in maintaining confidentiality during an investigation. Members who require a laptop with aircard to complete the investigation shall contact MISD Help Desk, upon APPROVAL of investigation, and provide required information.

In addition to using a Department laptop with aircard, members of the service are urged to take the following precautionary measures:

a. *Avoid the use of a username or password that can be traced back to the member of the service or the Department;*
b. *Exercise caution when clicking on links in tweets, posts, and online advertisements;*
c. *Delete "spam" email without opening the email; and*
d. *Never open attachments to email unless the sender is known to the member of the service.*

Furthermore, recognizing the ease with which information can be gathered from minimal effort from an Internet search, the Department advises members against the use of personal, family, or other non-Department Internet accounts or ISP access for Department business. Such access creates the possibility that the member's identity may be exposed to others through simple search and counter-surveillance techniques.

DEPARTMENT POLICY

The "Handschu Consent Decree" and "Guidelines for Investigations Involving Political Activity" (see Appendix "A" and "B" of Interim Order 58, series 2004, "Revision to Patrol Guide 212-72, 'Guidelines for Uniformed Members of the Service Conducting Investigations of Unlawful Political Activities'") require that any investigation, including investigations on social networks, by the New York City Police Department involving political activity shall be initiated by and conducted only under the supervision of the Intelligence Division. Accordingly, members of the service shall not conduct investigations on social networks involving political activity without the express written approval of the Deputy Commissioner, Intelligence. Any member of the service who is uncertain whether a particular investigation constitutes an "investigation involving political activity" shall consult with the Legal Bureau.

ADDITIONAL DATA (continued)	*Members of the service who have created and used online aliases prior to the promulgation of this procedure must submit a request to continue utilizing the alias in accordance with this procedure.*
RELATED PROCEDURES	*Citywide Intelligence Reporting System (P.G. 212-12)* *Guidelines for Uniformed Members of the Service Conducting Investigations of Unlawful Political Activities (Interim Order 58, series 2004)*
FORMS AND REPORTS	*Typed Letterhead*

3. Commanding officers will ensure that the contents of this Order are brought to the attention of members of their commands.

BY DIRECTION OF THE POLICE COMMISSIONER

DISTRIBUTION
All Commands