



Real-Time and Open Source Analysis

Examples of
Tools and Tradecraft

July 2017

Table of Contents

Resource Overview	1
Using ROSA for Criminal Investigative Support	2
Capabilities of ROSA Tools	3
Scenario-Based Examples	4
Scenario 1: Threat Made to a Judge	4
Scenario 2: Citizen Safety Concern.....	5
Scenario 3: High-Profile Visitor.....	6
Scenario 4: Strategic Collection of Open Source Information for Investigative Purposes.....	7
Items for Law Enforcement to Consider When Using ROSA	8
Online Alias Request Form Template	9
Online Undercover Activity Request Form Template.....	11
Request for Information Template	13

Resource Overview

The National Network of Fusion Centers (NNFC), in partnership with the Office of the Director of National Intelligence's (ODNI) Office of Partner Engagement-Information Sharing Environment (PE-ISE), the U.S. Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the associations represented on the Criminal Intelligence Coordinating Council (CICC), developed the *Real-Time and Open Source Analysis (ROSA) Resource Guide: Understanding and Using Open Source Resources for Law Enforcement Operations* (Resource Guide) to assist agencies and fusion centers in understanding the lawful and appropriate use of open source information, focusing on social media. It is designed to help law enforcement agencies and analytic personnel understand the potential tools and resources available to support law enforcement operations, while ensuring that related privacy, civil rights, and civil liberties (P/CRCL) concerns are addressed. The Resource Guide is publicly available but does not contain specific details on ROSA-related tools and tradecraft utilized by law enforcement and analytic personnel. Therefore, the supplemental product *Real-Time and Open Source Analysis (ROSA): Examples of Tools and Tradecraft* (Tools and Tradecraft) was created to highlight operational uses for state and local law enforcement analytic personnel by providing useful examples of tradecraft and tools utilized in the field for criminal intelligence product development and criminal case support. In addition, several scenarios are provided to help demonstrate the use of ROSA to showcase a threat-driven, tactical approach to open source analysis.

The Resource Guide and Tools and Tradecraft document focus on the social media component of real-time and open source analysis (ROSA). ROSA is the process conducted by law enforcement and analytic personnel to (1) develop or enhance criminal intelligence (including situational awareness reports), (2) support a criminal investigation, or (3) identify public safety risks either past, present, or anticipated. During the ROSA process, law enforcement and analytic personnel gather publicly available information (otherwise known as open source) via social media resources and tools for analysis to determine whether criminal activity is occurring to support a criminal investigation or to assess risks to public safety and security.

For purposes of this guidance, references to "social media" include only publicly available information derived from social media sites. The document is not intended to cover legal or policy issues related to accessing private social media information.

Using ROSA for Criminal Investigative Support

ROSA, as a part of criminal investigative support, can be valuable to successfully initiating, conducting, and completing investigations. For example, ROSA can be utilized to identify criminal suspects, evidence pertinent to a criminal investigation, and possible witnesses of a criminal act and other criminal-related activities.

ROSA, as a part of investigative support, can:

1. Include criminal subject background information: ROSA can be used by analysts to assist in more fully developing information on criminal suspects. Analysts may access social media resources and tools to identify social media "handles" and gather information related to a criminal subject, including potential criminal associates, pictures, and other activities related to the criminal activity.
2. Determine historical and recent online activities and develop timelines: As a part of a criminal investigation, it is important to identify timelines. Social media resources and ROSA-related activities can be used by analysts to develop timelines of suspects or criminal activity or the last known activities of victims.¹
3. Identify criminal associates: Analysts may use ROSA to identify potential criminal associates by the identification and analysis of "friends," "followers," or "associates" who are reasonably suspected of criminal activity. It is important to note that merely "following" someone on a social media site does not necessarily mean that there is an identified criminal relationship. Analysts and law enforcement personnel should be cautious of linking subjects because of a social media relationship unless a criminal nexus can be supported by clearly articulated, factual information.¹
4. Identify additional incidents as part of a criminal trend or pattern: Analysts should use ROSA and social media searches to assist in developing crime trends and patterns activity. If a robbery were to occur at a convenience store, analysts should look at social media to identify whether there are any additional videos of the incident, any witnesses who may have left the crime scene, or any similar incidents in the area, within a related time frame.
5. Identify a possible suspect(s): ROSA can support the identification of possible criminal suspects. If someone posts a video of criminal activity, ROSA may be used to capture images of the criminal suspect(s) as lead information used to identify the name of the suspect.

¹ In some instances, a description of individuals or groups who are victims or targets of violence must be included to provide necessary context for investigation of an illegal act. These persons or groups should be clearly identified as victims or witnesses, etc. See *Privacy, Civil Rights, and Civil Liberties Audit Guidance for the State, Local, Tribal, and Territorial Intelligence Component* (Sept. 2015), <https://www.it.ojp.gov/GIST/181/Privacy--Civil-Rights--and-Civil-Liberties-Audit-Guidance-for-the-State--Local--Tribal--and-Territorial-Intelligence-Component>.

Capabilities of ROSA Tools

ROSA tools have a wide variety of capabilities and cost, and law enforcement agencies should understand the needs of their analysts and investigators before deciding which tools are best for their organization. Many of these tools may have one or more of the following capabilities:

- One-click translation—Select text in a foreign language and convert it to English and vice versa.
- Geofencing—Search a certain area for designated key words.
- Geolocation—Search designated key words and see the probable location of the individual who posted the related message online.
- Social media aggregation—Search multiple social media platforms through basic and advanced queries.
- Global key word—Search designated key words within all public posts.
- Word clouds—An image composed of various words, in which the presence and size of each word is based on its frequency in use across a specific sampling of posts.
- Sentiment analysis—Interpreting whether a post has a positive, negative, or neutral tone based on analyzing the text contained within the post.

A well-rounded open source analysis capability will incorporate the use of multiple ROSA tools in order to compensate for any particular ROSA tool limitation. Some examples of limitations include (1) a search shows results only if a user's post is geotagged, which users can disable; (2) not including a multilingual search capability; (3) extensive setup before initial deployment; or (4) various collection limitations, such as a search tool that is able to pull information from only a small percentage of social media sites.

Because of rapidly changing technology, the capabilities of ROSA tools can suddenly change. For example, an aggregation software company receives access to a social media platform through an agreement with that social media company. If the social media company decides to discontinue the software company's access, the capabilities of that software are greatly diminished. Also, social media sites are shut down, new ones emerge, and some new capabilities may even conflict with law enforcement authorities. Therefore, law enforcement agencies should regularly assess the tools available; confirm that the use of such tools is consistent with applicable law, regulation, and policy; and evaluate the impact of the new capabilities and/or tools on P/CRCL. In addition to this list of tool capabilities, law enforcement agencies may reach out to state or major urban area fusion centers in their area of responsibility for additional information on ROSA.

Scenario-Based Examples

The following scenario-based examples are intended to outline steps that law enforcement personnel may take to utilize open source analysis during various situations.

Scenario 1: Threat Made to a Judge

The following scenario involves multiple law enforcement jurisdictions and fusion centers and outlines a scenario that could possibly occur following a controversial public activity.

- A Superior Court judge in San Francisco, California, issues a controversial decision that receives substantial media attention. Local fusion center analysts are aware of the decision and remain alert to online activity related to the situation.
- A man in Orlando, Florida, sees the following comment made by an individual about the judge on his social media feed: "Judge Doe #DeadJudge" and a gun emoji.
- He takes a screen shot of this comment and sends the PDF of the comment to local law enforcement, who forward the information to their local fusion center.
- A fusion center analyst conducts open source research to determine whether or not the threat is credible. She begins with the individual's social media username, which is indicative of the person's first and last name, so she considers it PII and takes the necessary precautions. Based on her search, it is believed that the individual lives in Denver, Colorado. After additional research, the analyst finds a Facebook page that appears to be the same individual. On the page, the user mentions that he will be traveling the next day to San Francisco, California, where the judge works. The analyst also finds a post from two days ago on the user's page stating: "Judge Doe wants to take away our living rights . . . so I'll take away his right to live . . ."
- The fusion center analyst saves the Facebook page as a PDF and notes any other websites researched and what was and was not found and forwards the information to tactical law enforcement, the California fusion center, the Colorado fusion center, and appropriate agencies in these areas, so all parties are aware of the situation.
- The fusion center analyst in Florida sends a notification to appropriate sworn law enforcement personnel in the area of responsibility to investigate the threat and attempt to locate the individual.
- The fusion center analyst in California receives the information and conducts further research, discovering that the same individual made a more recent threat to the judge on his social media page. The fusion center analyst in California produces a situational awareness bulletin and disseminates it to local law enforcement, courthouse security personnel, and any other partners with a need to know.

Scenario 2: Citizen Safety Concern

The following scenario outlines a situation involving the safety of community members.

- A high school student near Madison, Wisconsin, is on a popular social media site that allows users to easily post short videos.
- The student sees a video posted by a social media user stating that he wants to commit suicide and notices that someone going by the same username also posted a picture of his suicide letter.
- The student notices that several people have commented asking the person to not go through with it, but there has been no response from the user.
- The student takes a screen shot of the photograph and sends the image to the local law enforcement agency. The agency then sends a request for information (RFI) to the state fusion center, seeking information about the identity and location of the possibly suicidal teen. The social media content pertaining to the user is included in the RFI. The information in the RFI is considered PII, and the necessary precautions are taken.
- A fusion center analyst conducts open source research to try to identify the location and identity of the user as a matter of public safety. The analyst's research reveals a match to a profile that provides additional information on the individual, including his location in the vicinity of Seattle, Washington.
- The fusion center analyst in Wisconsin saves the social media profile page as a PDF and provides the information to local law enforcement officers.
- Local law enforcement immediately informs the local law enforcement in Seattle of this individual and his threats to kill himself.
- Local law enforcement personnel are able to identify an address associated with the suicidal individual's name and determine that he is 15. A patrol officer is sent to the address to conduct a welfare visit.
- The suicidal teen's mom answers the door, and she is unaware of her son's threats to take his own life.
- The mom and officer go to the teen's room and find him unresponsive.
- The officer radios for an ambulance, which arrives in time to save the teen's life.

Scenario 3: High-Profile Visitor

The following scenario involves the safety of a high-profile individual and community members during a large-scale event.

- The current pope is on a visiting tour of several U.S. cities, and one of his stops is Philadelphia, Pennsylvania.
- Prior to and during the visit, the local fusion centers analyzed open source information for situational awareness, with an emphasis on identifying potential threats to the pope, individuals, and the event itself.
- A fusion center analyst uses several key words related to the event to review open source information, including *kill*, *sniper*, *die*, and *pope*, in an effort to detect and identify individuals who are planning to engage in or are engaging in criminal activity related to the event.
- The analyst sees a public post of a picture of a white male holding a butcher knife, with the caption "When you protectin' yoself, but the snipers bout to hit." The analyst recognizes the background of the picture as the inside of the secure zone, in close proximity to the pope.
- As the analyst is reviewing the individual's social media page, he posts a picture of a cardboard sign written in black marker that says "DON'T TOUCH! Jesus and the pope and the SNIPERS are watching," with a comment that says "Watcha gon' do when they come for you? #ThatWillTeachYou #DontTouch" and that includes emojis of a church and a gun.
- The analyst is able to use information on the individual's social media account to search a law enforcement-only access portal, which produced a potential first and last name.
- The analyst then enters the information gleaned from the individual's social media account into a social media aggregating software, which gave an exact location of the individual because his Global Positioning System (GPS) coordinates were turned on.
- The analyst compares some photographs from the individual's social media account to those in the law enforcement-only access portal and determines them a positive match.
- At this point, the analyst has a positive ID on the individual, including a photograph, an address, and the exact location for the individual inside the papal secure zone. The analyst forwards the information to on-site security personnel.
- On-site security personnel locate the individual, who is a vendor working at a food stand for a local popular restaurant. The man had a picture taken with a butcher knife because he was setting up and preparing to cook meals.
- The entire vetting process to clear this individual of any criminal acts was less than 15 minutes.
- Given the absence of a valid law enforcement (including public safety) purpose, the information was purged from the system in accordance with agency policy.

Scenario 4: Strategic Collection of Open Source Information for Investigative Purposes

The following scenario involves the proactive use of open source resources to identify potential threats to public safety personnel and/or community members.

- Following an increase in incidents of violence towards law enforcement officers nationwide, a fusion center tasks an analyst with reviewing real-time and open source information for combinations of key words, such as “kill” and “cop.”
- The search leads the Washington Regional Threat Analysis Center (WRTAC) analyst to a public social media account where the user recently posted, “My whole life has led me to this point. Time to kill a cop.” The analyst then conducts additional research in an attempt to determine whether there is a credible threat.
- The WRTAC analyst searches past posts on the user’s account and finds one that states, “cop killer and proud of it.” The individual’s username on the account is not an identifiable name, so further analysis is necessary.
- The account holder had posted a photo of himself and some other identifiable landmarks on his account, such as tagging himself at a restaurant with the comment “I’m taking on the Big Bob Eating Challenge! Haven’t tried this since freshman year at UC!”
- The analyst searches “pizza” and “Big Bob Eating Challenge” and finds a possible match in Cincinnati, Ohio.
- At this point, the WRTAC analyst has a possible photo of the subject and a town that the person frequents and believes that the person attends or has attended the University of Cincinnati (UC).
- The WRTAC analyst contacts the Greater Cincinnati Fusion Center (GCFC) and sends a PDF of the subject’s social media page, along with the photograph and other details, to a GCFC analyst. The GCFC analyst forwards the information to the Cincinnati Police Department (CPD) and University of Cincinnati Police Department (UCPD).
- The CPD and UCPD coordinate resources and identify the subject as a current UC student living on campus. The subject was detained for making threats to law enforcement, and a search warrant of his dorm room produced several types of narcotics and a firearm.

Items for Law Enforcement to Consider When Using ROSA

- Is the threat information credible? Is there a potential threat or risk to public safety?
- What are the applicable state and local criminal laws that prohibit true threats?
- Was the threat general or more specific?
 - One general threat with no other signs of violent behavior may not be a credible threat to investigate further. More specific threats or multiple threats of violence are more credible.
- Does the individual have a history of violent behavior?
 - If the individual makes more than one threat on social media and there is criminal predicate to run the person through an internal law enforcement database(s) and perform a criminal history check and a history of violent behavior is identified, this information needs to be included in the summary. The summary should state whether an open source check revealed any other relevant information about this individual (e.g., other threatening comments made by the individual, pictures, activities and/or associations).
- Is PII collected, used, stored, or disseminated, and if so, what are the necessary privacy protections that should be put in place per agency policy?

Online Alias Request Form Template

INSERT IMAGE HERE

Online Alias Request Form

INSERT IMAGE HERE

The purpose of this form is to request authorization to develop an online alias in accordance with the [AGENCY] Use of Real-Time and Open Source Analysis Policy.

An online alias may be used only to monitor activity on social media websites and only in accordance with the [AGENCY] Use of Social Media Policy.

All online alias requests will be retained for a period of two years from the date of deactivation or denial. It shall be the responsibility of the immediate supervisor to update the status of the online alias [LOCATION WHERE SAVED] if it has been deactivated. [AGENCY] personnel are also responsible for notifying their immediate supervisor if they have deactivated their approved online alias.

Without prior authorization, personnel are prohibited from using an online alias for undercover activity, which is defined as engaging and interacting with others online. For authorization to use an online alias for an undercover purpose, the Online Undercover Activity Request Form must be used. (Refer to the [AGENCY] Use of Social Media Policy for more information.)

Requestor Name:		Request Date:	
Requestor's Position:		Phone Number:	
Immediate Supervisor:		E-Mail Address:	
Employee Assignment:		Case Number (If Applicable):	
Operation Name (If Applicable):			

Identity and/or background information to be utilized for the online alias

Purpose for online identity:

--

Alias Name:		Social Media Accessed:		Image/Avatar Used
Sex:		Social Media Accessed:		
DOB:		Social Media Accessed:		
Username or E-Mail:		Social Media Accessed:		

Online Alias Request Form
Page -1-

Other information for online identity: Other social media, physical addresses, employment, special interests, personal or professional affiliations, or any other background information that is anticipated to be required as part of the process to establish the online alias.

I hereby acknowledge that I have reviewed the [AGENCY] Use of Real-Time and Open Source Analysis Policy. I also acknowledge that the use of this online alias will be based only upon a criminal predicate or threat to public safety or based upon reasonable suspicion that an identifiable individual, regardless of citizenship or U.S. residency status, or organization has committed an identifiable criminal offense or is involved in or is planning criminal conduct or activity that presents a threat to an individual, the community, or the nation and the information is relevant to the criminal conduct that is related to crime analysis, situational assessments/awareness, developing criminal intelligence, or supporting a criminal investigation.

Applicant Signature:

Supervisor Review:

Deputy Director Approval:

Alias Activation Date:

Denial/Deactivation Date:

Purge Date:

Online Undercover Activity Request Form Template

INSERT IMAGE HERE

Online Undercover Activity Request Form

INSERT IMAGE HERE

The purpose of this form is to request authorization to utilize an online alias to engage and interact with persons via social media websites in accordance with the [AGENCY] Use of Real-Time and Open Source Analysis Policy.

Online undercover activity may be utilized only when there is reason to believe that criminal offenses have been, will be, or are being committed (e.g., Internet chat rooms where child exploitation occurs). Online undercover activity must have a valid law enforcement purpose and may be used only in accordance with the [AGENCY NAME AND POLICY].

All online alias requests will be retained for a period of two years from the date of deactivation or denial. It shall be the responsibility of the immediate supervisor to update the status of the online alias [WHERE INFORMATION SAVED] if it has been deactivated. Immediate supervisors must also review online undercover activity on a weekly basis to ensure continued need. Approved online undercover activity that does not provide pertinent information related to valid law enforcement purpose within thirty (30) days will be discontinued.

This form should not be used to authorize real-time and open source analysis (ROSA). For ROSA authorization, use the Online Alias Request Form. Under exigent circumstances, the unit supervisor may obtain via chain of command verbal authorization for online undercover activity (refer to the [AGENCY AND POLICY NAME] policy for more information).

Requestor Name:		Request Date:	
Requestor's Position:		Phone Number:	
Immediate Supervisor:		Employee Assignment:	
Enforcement Agency Supported:		Case Name/Number:	

Purpose and anticipated duration for online identity:

Identity and/or background information to be utilized for the online alias

Alias Name:		Social Media Accessed:		Image/Avatar Used
Sex:		Social Media Accessed:		
DOB:		Social Media Accessed:		
Username or E-Mail:		Social Media Accessed:		

Online Undercover Identity Request Form
Page -1-

Other information for online identity: Other social media, physical addresses, employment, special interests, personal or professional affiliations, or any other background information that is anticipated to be required as part of the process to establish the online alias.

--

I hereby acknowledge that I have reviewed the [AGENCY] Use of Real-Time and Open Source Analysis Policy. I also acknowledge that the use of this online alias will be based only upon a criminal predicate or threat to public safety or based upon reasonable suspicion that an identifiable individual, regardless of citizenship or U.S. residency status, or organization has committed an identifiable criminal offense or is involved in or is planning criminal conduct or activity that presents a threat to an individual, the community, or the nation and the information is relevant to the criminal conduct that is related to crime analysis, situational assessments/awareness, developing criminal intelligence, or supporting a criminal investigation.

Applicant Signature:

--

Supervisor Review:	
Deputy Director Approval:	
Alias Activation Date:	☐ Deconfliction? (SYSTEM NAME)

30-Day Validation Date:	
Denial/Deactivation Date:	
Purge Date:	

Request for Information Template

On DATE/TIME, Officer NAME from the AGENCY requested that the FUSION CENTER NAME review real-time and open source information regarding INSERT DESCRIPTION HERE].

As a result, the FUSION CENTER NAME requests to use real-time and open source analytical tools to identify any potential threats to INCIDENT OR EVENT. *[This is related to information received by the AGENCY that THREAT DESCRIPTION.]* FUSION CENTER NAME will use real-time and open source information to analyze evidence that is relevant to criminal activity, planned criminal disruptions, direct or implied threats of violence, or other criminal conduct in regards to this event or incident.

Analysts at FUSION CENTER NAME will begin the review on DATE and will be utilizing the following tools for a general review of real-time and open source information:

FUSION CENTER NAME will use real-time and open source analysis and tools to review and identify any potential threat information, as described above. FUSION CENTER NAME will not retain any information that is found in the course of the review, unless such information is relevant to criminal activity, planned criminal disruptions, direct or implied threats of violence, or other criminal conduct in regards to this event or incident. If criminal threat information is found, FUSION CENTER NAME will disseminate the information to the appropriate law enforcement and public safety entities in a timely manner and will retain that information in accordance with the retention period determined by the system in which the information is stored.

FUSION CENTER NAME will cease this review on DATE.