



Real-Time and Open Source Analysis Resource Guide

Understanding and Using
Open Source Resources for
**Law Enforcement
Operational and
Analytic Activities**

July 2017

ROSAS

Overview of the Real-Time and Open Source Analysis Resource Guide

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 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 operational and analytic activities, while ensuring that related privacy, civil rights, civil liberties (P/CRCL) concerns are addressed.

The resource guide addresses several key areas that will help law enforcement and analytic personnel use ROSA, including:

- ◆ Capabilities of ROSA tools
- ◆ Considerations for using ROSA for the development of criminal intelligence, investigative support, and public safety
- ◆ Deconfliction of threat information
- ◆ Dissemination of ROSA-related information or criminal intelligence
- ◆ P/CRCL considerations for ROSA criminal intelligence and investigative support
- ◆ Operational security
- ◆ Reevaluation of policies, procedures, products, and resources
- ◆ ROSA-related training topics and examples
- ◆ Recommended practices for law enforcement and analytic personnel using ROSA

There are an ever-increasing number and variety of ROSA tools and resources. Many of the elements set forth in this resource guide can be applied to all open source resources, and agencies should regularly review the ROSA resources accessed and used by personnel within the agency.



Real-Time and Open Source Analysis Resource Guide

Understanding and Using
Open Source Resources for
**Law Enforcement
Operational and
Analytic Activities**

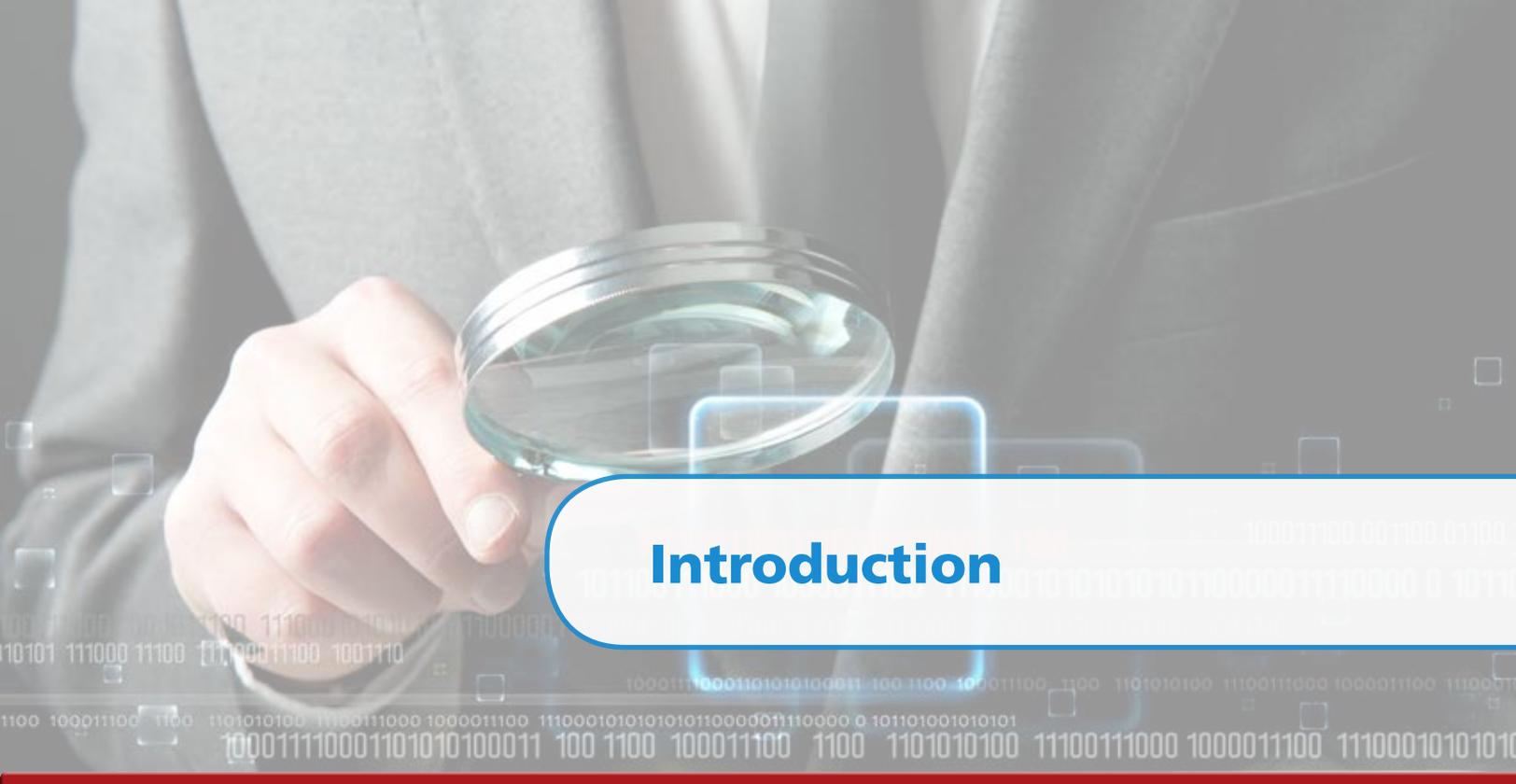
July 2017

Contents

Introduction	1
Capabilities of ROSA Tools	3
Using ROSA for the Development of Criminal Intelligence, Investigative Support, and Public Safety	5
Privacy, Civil Rights, and Civil Liberties Considerations	9
Operational Security	13
Deconfliction	15
Dissemination of ROSA-Related Information or Intelligence	17
Reevaluation of Existing Policies, Procedures, Products, and Resources	19
ROSA-Related Training	21
Recommended Practices for Law Enforcement and Analytic Personnel Using ROSA	23
Endnotes	25
Appendices	
Appendix I—ROSA-Related Terms and Definitions	29
Appendix II—ROSA-Related Case Law and Guidance	33
Appendix III—ROSA Considerations and Common Practices Related to PII	37
Appendix IV—Fair Information Practice Principles	39
Appendix V—Additional Resources	43



It is important that agencies develop a framework for using open source analysis and sharing cyber-related information while protecting individuals' privacy, civil rights, and civil liberties.



Introduction

Law enforcement agencies and fusion centers have the responsibility to protect and serve. This responsibility comes from the legal authority to enforce applicable local, state, and federal criminal statutes focusing on the damage to or loss of personal property and threats to personal safety and well-being. State, local, tribal, and territorial (SLTT) law enforcement and analytic personnel work hard to both prevent crimes before they occur and solve crimes when perpetrated. Traditionally, law enforcement agencies have two avenues to do so—the development and use of criminal intelligence and the conduct of criminal investigations. A resurgence of the value and use of criminal intelligence has occurred since the terrorist attacks on September 11, 2001, through the release of the *National Criminal Intelligence Sharing Plan (NCISP)* (Version 1¹ and Version 2²). The NCISP emphasizes the value and role of all police agencies to use their authorities to develop intelligence, particularly criminal intelligence information,³ on individuals and organizations reasonably suspected of being involved in criminal activity and the adoption of 28 CFR Part 23 as the accepted standard for doing so.⁴

Criminal intelligence operations and criminal investigative activities of law enforcement and

This document focuses 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.

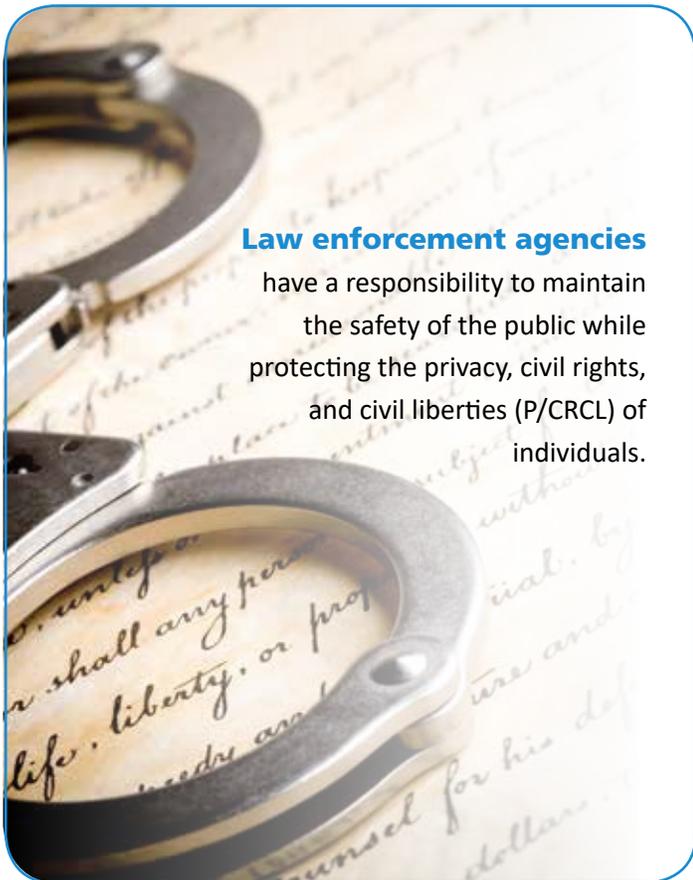
For purposes of this guidance, references to “social media” include only publicly available information derived from social media sites. The document is not intended to cover legal or policy issues related to accessing private social media information.

analytic personnel depend on a wide array of sources and information. These include investigative procedures, such as interviews; obtaining information through judicial authorization, such as search warrants and subpoenas; and information obtained through what are recognized as open sources. In recent years, one type of open source information—publicly available information derived from social media, as opposed to information not generally available to the public because of user privacy settings or social media platform functionality—has emerged as a valuable source of information for law enforcement and analytic personnel in its crime prevention and response role. SLTT law enforcement and analytic personnel may, when authorized and appropriate, use publicly

available information, including social media, as a part of their development of situational awareness reports or actionable intelligence. With the advent of social media and its new technologies, it is important that law enforcement agencies and fusion centers understand how to appropriately and lawfully access and use publicly available information.⁵

To assist law enforcement and fusion center personnel in understanding how to effectively use this type of open source information that is often available in real time, this resource guide has been developed by stakeholders from state, local, and federal law enforcement. The guide focuses on law enforcement and analytic personnel, providing guidance and resources to better understand how to analyze publicly available open source information, focusing on social media, for criminal intelligence, investigative support, and public safety support, while operating in accordance with their organization’s legal and policy constraints. For the purposes of this document, this analysis effort is referred to as real-time and open source analysis (ROSA).

The primary audience for this resource guide is law enforcement and analytic personnel performing an open source analytic function in support of public safety agencies. Law enforcement and analytic personnel can use this resource guide to better understand how to appropriately use open source information derived from publicly available sources, including social media, for criminal intelligence development or investigative support, as it relates to their authorities. In addition to law enforcement and analytic personnel, supervisors or agency leadership may use this resource to help understand policies and procedures that should be in place for agency and fusion center personnel to appropriately use open source information derived from social media, as well as the value of ROSA in agency operations.



Law enforcement agencies

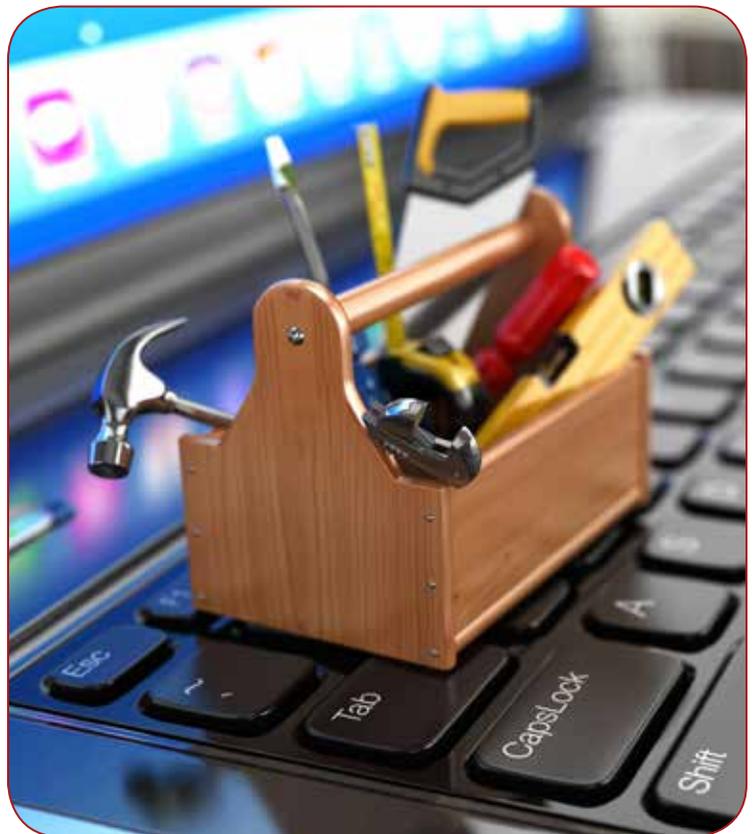
have a responsibility to maintain the safety of the public while protecting the privacy, civil rights, and civil liberties (P/CRCL) of individuals.



Capabilities of ROSA Tools

Open source platforms can be used by criminals to instigate or conduct illegal activity and by terrorists to recruit and encourage new members, disseminate violent extremist messaging through video or documents, coordinate activities, and claim responsibility for attacks around the world. As such, law enforcement and analytic personnel should understand the uses of social media and be aware of social media tools that can be used to document criminal and terrorist activity. A wide variety of open source analysis tools—both no-cost and paid—is available to public and private sector organizations, including law enforcement and analytic personnel, and the technology continues to evolve. ROSA tools that access only publicly available information and are capable of searching multiple platforms simultaneously are assets for maximizing efficiency during authorized uses by law enforcement and analytic personnel.

Law enforcement agencies and fusion centers should regularly assess the tools available; understand, to the extent possible, how the tools work before employing them; confirm that the use of such tools is consistent with applicable law, regulation, and policy; require human review of any search results returned by an automated or semiautomated tool; and evaluate the impact of the new capabilities



and/or tools on P/CRCL. Law enforcement agencies may reach out to state or major urban area fusion centers in their area of responsibility for additional information on ROSA tools and capabilities.



Using ROSA for the Development of Criminal Intelligence, Investigative Support, and Public Safety

It is incumbent on SLTT law enforcement agencies and fusion centers to ensure that their use of ROSA is authorized by applicable law, regulations, policies, and procedures and is conducted in a manner that appropriately protects privacy, civil rights, and civil liberties (P/CRCL).⁶ When considering the collection and use of open source information, law enforcement and analytic personnel should consider that the vast majority of content and personal connections revealed will be constitutionally protected activity. Law enforcement and analytic personnel should therefore understand that their legal authority to gather and use open source information will depend on whether they have a valid law enforcement (including public safety) purpose and a defined job responsibility to gather and analyze open source information. They may use ROSA to assist their agency or fusion center with effectively accomplishing its mission of protecting the public. Consider the following uses of ROSA:⁷

- ◆ Detection of criminal activity, including potentially violent situations or threatening behavior
- ◆ Assessment of threats to the public or critical infrastructure
- ◆ Analysis of suspicious activity reports potentially related to terrorism



Identifying Threatening Communications

While ROSA has many applications, its use as a means for identifying threatening communications raises some issues. Law enforcement and analytic personnel are encouraged to coordinate with their legal representatives to familiarize themselves with their local and state criminal law(s) that prohibit “true threats.”⁸ The term *true threats* refers to “those statements where the speaker means to communicate a serious expression of an intent to commit an act of unlawful violence to a particular individual or group of individuals.”⁹ Although the First Amendment to the U.S. Constitution guarantees the right to free speech, this right does not extend to true threats. The statutory schemes for charging offenses related to true threats vary from state to state. By way of example and depending on the jurisdiction, the offense may be charged as a criminal threat, a terroristic threat, communicating threats, or harassment/stalking, among other ways.

For a discussion about the First Amendment considerations related to true threats and political advocacy, refer to page 9. For examples of ROSA-related case law and guidance, see Appendix II.

- ◆ Acquisition of physical evidence related to a crime
- ◆ Identification of victims and suspects of a crime
- ◆ Natural disasters or other emergency management operations

When information on a potential threat to law enforcement or public safety is discovered or received by SLTT law enforcement and analytic personnel, law enforcement is encouraged to evaluate the credibility of the threat information or to assess the potential threat or risk to public safety, examining the source reliability and content validity of the information. When a threat

has been evaluated and the applicable requirements for a threat have been met, (subject to the First Amendment),¹⁰ law enforcement and analytic personnel are then able to conduct additional research and analysis to supplement ROSA.

SLTT law enforcement and analytic personnel may access and leverage different types of information and intelligence¹¹ and a variety of intelligence products, in accordance with a valid law enforcement purpose—articulated in internal policies—and a defined job responsibility. Once open source information is accessed by law enforcement and analytic personnel and

Common Practices Related to Analyzing Open Source Information

The following common practices can assist law enforcement and analytic personnel in analyzing open source information:

Evaluate source reliability and content validity.

Confirm that the use of ROSA is consistent with the agency's privacy policy and/or ROSA policy.

Evaluate the content of the threat and assess the significance and potential risk associated.

Confirm that the use of ROSA is authorized under agency authorities and is consistent with applicable laws, regulations, and policies.

Check the information against appropriate law enforcement indices as determined by the level of suspicion required for such action.

Assess open source information against current threat reporting, including documented SLTT and federal situational awareness, warnings, and notices.

incorporated into a criminal intelligence or investigative file, it is important to understand that the information is then considered investigative or criminal intelligence information and that the laws, regulations, and policies applicable to that type of information or intelligence govern its use, retention, and sharing.

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:

- ◆ Include criminal subject background information
- ◆ Determine historical and recent online activities of suspects and victims
- ◆ Identify additional incidents as part of a criminal trend or pattern
- ◆ Identify a possible suspect(s) or associate(s)

Situational Awareness, Criminal Intelligence Information, and Intelligence Products

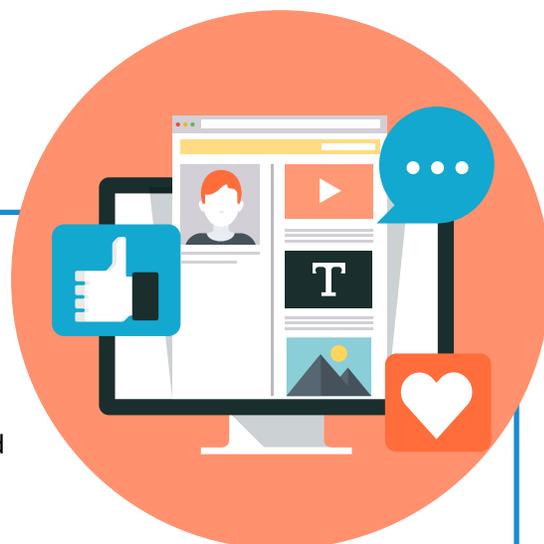
As a part of an agency's vetting and intelligence function, ROSA may be utilized to identify individuals and organizations that are reasonably suspected of involvement in criminal activity under 28 Code of Federal Regulations (CFR) Part 23 and used to support the development of strategic and tactical intelligence products to identify potential threats, public safety hazards, incidents, and crime trends. SLTT law enforcement and analytic personnel may use open source analysis to develop situational awareness reports or actionable intelligence. When applying a strategic approach to ROSA, SLTT law enforcement and fusion centers should consider specific information needs or intelligence gaps. Strategic and tactical ROSA can also be conducted to support an active event or ongoing incident with first responder deployment and is often done in real time. When

conducting this type of ROSA, SLTT law enforcement and analytic personnel should consider the evolving public safety environment, have a valid law enforcement purpose, and incorporate the operating principles of 28 CFR Part 23, as appropriate, as a part of their broader intelligence development mission.

For law enforcement and analytic personnel who focus on the development of criminal intelligence, ROSA can be used in a number of ways:

- 1. Situational awareness reports:** Law enforcement and analytic personnel may use ROSA to develop and/or enhance situational awareness reports. Social media can provide a useful tool to identify trends within an area or trends about a specific activity. This information can then be used to build, inform, or enhance situational awareness reports.
- 2. Criminal/terrorism analysis and criminal intelligence development:** Law enforcement and analytic personnel who focus on the development of criminal intelligence may also use ROSA as a part of their collection and analysis of criminal activity. For suspects who are reasonably believed to be conducting preoperational planning for a crime, including a terrorist attack, an analyst may search social media sites to identify activities of the suspect, corroborate reporting, and identify potential criminal associates.
- 3. Suspicious activity reporting (SAR) analysis:** ROSA can provide beneficial support to agencies that gather, analyze, and disseminate information related to the SAR process. Law enforcement and analytic personnel may use social media tools to identify suspicious behavior, capture and collect this information, and analyze it for trends within a jurisdiction or analyze it to determine whether it documents observed behavior reasonably indicative of preoperational planning associated with terrorism or other criminal activity.¹²

Example—ROSA for Criminal Intelligence Development



On November 28, 2016, at Ohio State University (OSU) in Columbus, Ohio, an individual drove a car into a group of people and then exited the vehicle and began slashing bystanders with a knife. The attacker was fatally shot soon after, and while law enforcement officers were securing the area and helping victims, authorities worked to identify the suspect. What followed was a nationwide dragnet for information, including homeland security partners at the federal, state, and local levels.

Authorities found a driver's license with the name of a possible suspect. The information was sent to the Strategic Analysis and Information Center in Columbus, Ohio, and shortly after, an analyst at the center was able to use open source analysis to locate the suspect's Facebook page. The fusion center analyst identified an important piece of evidence through open source analysis, which was used to further support the identification of the subject and/or acquaintances. The analyst disseminated the Facebook page to other fusion centers and state and federal partners, including the local Federal Bureau of Investigation (FBI) Joint Terrorism Task Force (JTTF).

The article is available at <http://abcnews.go.com/US/suspected-terror-attack-osu-launched-nationwide-dragnet-information/story?id=44056937>.



Privacy, Civil Rights, and Civil Liberties Considerations



General Legal Concepts

Law enforcement and analytic personnel must interpret the law(s) in their jurisdiction that cover criminal activity, including threats in a manner that is consistent with the First Amendment to the U.S. Constitution.¹³ When interpreting the applicable penal code, law enforcement and analytic personnel must distinguish between criminal conduct and lawful speech. For example, under the First Amendment, a threat statute must be interpreted to cover only a “true threat” and not “constitutionally protected speech.”¹⁴ The speaker need not actually intend to carry out the threat.¹⁵ A true threat “must convey a serious or genuine threat, and must be distinguished from idle, careless talk, exaggeration, jests, or political hyperbole.”¹⁶

In contrast to a “true threat,” the First Amendment protects political hyperbole and “vehement, caustic, and sometimes unpleasantly sharp attacks” that do not rise

to the level of a true threat.¹⁷ Context is paramount in distinguishing between true threats and protected speech.¹⁸ It is recommended that law enforcement and analytic personnel engage their agency’s legal counsel when analyzing true threats and First Amendment-protected speech.¹⁹

In addition, advocacy of violence or lawbreaking, depending on context, may be protected speech under the First Amendment, and as such, consultation with agency legal counsel is encouraged. For speech advocating violence or lawlessness to be unprotected, it must be directed at inciting “imminent lawless action” and be likely to produce the intended lawlessness or violence.²⁰ The likelihood of the intended violence must also be imminent, while the “advocacy of illegal action at some indefinite future time” may not suffice.²¹ Even though some speech may appear threatening, if the analysis in its totality demonstrates that the speaker generally advocates nonviolence or that the audience receiving the statements does not consider the speech to be threatening, then the statements—however crude or unartful—may still be protected by the First Amendment.²²

On the other hand, given the right context, language can be considered threatening. Speech may lose its protection when it is used to intimidate others.²³



a proposal to engage in illegal activity and the abstract advocacy of illegality.”²⁶

Law enforcement and analytic personnel should rely on their training and experience and engage their agency’s legal counsel for guidance when analyzing whether the expression constitutes criminal conduct or is a protected activity.

For further information on ROSA-related case law and guidance, see Appendix II.

Privacy, Civil Rights, and Civil Liberties Protection Policy

When used as a law enforcement tool to investigate and prevent criminal activity, ROSA must be used in a manner that adheres to the same principles that govern all law enforcement activity. Law enforcement agencies and fusion centers are encouraged to develop a policy with their agency’s legal counsel that defines and articulates the legal requirements that enable gathering and sharing of open source information to occur in a manner that protects the P/CRCL of individuals. This policy will guide investigative efforts and mitigate potential P/CRCL risks.

As outlined in the resource *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities—Guidance and Recommendations*, a comprehensive ROSA policy should include the following key components:²⁷

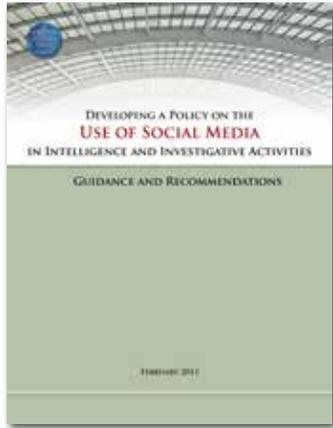
1. Articulate that the use of resources will be consistent with applicable laws, regulations, and agency policies and procedures.
2. Define if and when the use of open source platforms or tools is authorized (as well as use of information on these sites pursuant to the agency’s legal authorities and mission requirements).
3. Articulate and define the authorization levels needed to use information from open source platforms.
4. Specify that information obtained from open source resources will undergo evaluation to determine confidence levels (source reliability and content validity).
5. Specify the documentation, storage, and retention requirements related to information obtained from open source resources.

Language purely attempting to incite criminal activity, such as publicly proffering persons to harm those from an opposition group in exchange for compensation, will not likely be protected.²⁴ The U.S. Supreme Court has stated that “there remains an important distinction between

Terrorism-Related Issues

A recent Congressional Research Service report, *The Advocacy of Terrorism on the Internet: Freedom of Speech Issues and the Material Support Statutes*, discusses relevant precedent that may limit the extent to which advocacy of terrorism may be restricted. The report also addresses the potential application of the federal ban on the provision of material support to foreign terrorist organizations to the advocacy of terrorism and the dissemination of such advocacy by online service providers. The report has important insights for law enforcement intelligence that seeks to collect potential threat information about individuals who express support for a terrorism ideology.²⁵

6. Identify the reasons and purposes, if any, for off-duty personnel to use open source information in connection with their law enforcement responsibilities, as well as how and when personal equipment may be used for an authorized law enforcement purpose.



7. Identify dissemination procedures for intelligence and investigative products that contain information obtained from open source sites, including appropriate limitations on the dissemination of PII.²⁸ See Appendix III for further information about personally identifiable information (PII).

The following components are also integral and build on the recommendations of the *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities—Guidance and Recommendations*:

8. Understand the terms of service for open source platforms and tools that are used.
9. Limit the collection of publicly available social media information to that which is reasonably related to the purpose of the search.²⁹
10. Specify that social media should only be collected without regard to an individual's viewpoint or the fact of speaking itself, unless expressly relevant to the enforcement of a statute or regulation.

In addition, if the agency authorizes or intends to authorize online undercover activity (including developing an undercover profile on a social media site), the policy should address supervisory approval, required

documentation of activity, periodic reviews of activity, and the audit of undercover processes and behavior.

It is critical to understand that the presence of PII is the primary trigger for the privacy protections in an agency's P/CRCL and ROSA policies. Therefore, a ROSA policy should articulate how a law enforcement agency or fusion center handles PII and other personal, sensitive information it seeks or receives while conducting open source analysis and state also that personnel must have a defined objective and a valid law enforcement purpose for gathering, maintaining, or sharing PII.

It is also important to note that some information that may first appear not to be PII can be PII if it is linked or is linkable to a specific individual or if it may allow a specific individual to be identified when combined with other data. For example, a social media username that appears generic may actually be PII if it can be linked to a specific individual or if that same username is on a different social media platform that also includes an individual's photograph. Out of an abundance of caution, treat a username as if it is PII unless law enforcement or analytic personnel can show that the username is not linkable. Further information on recommended practices when using open sources is available on page 23.

A policy for using open source resources can be a stand-alone document or be incorporated as an appendix to an existing policy, such as a fusion center's P/CRCL policy or standard operating procedures (SOP).³⁰ It is important to seek review of the open source policy by legal and policy professionals, such as a privacy officer and agency legal counsel, prior to its issuance.³¹ Once an open source policy is in place, agencies should regularly review and update their policies and procedures, as appropriate. Additional information on developing a P/CRCL policy is available in *Fusion Center Privacy Policy Development: Privacy, Civil Rights, and Civil Liberties Policy Template*.³²



Operational Security

Law enforcement and analytic personnel connecting to an online environment, including accessing publicly available real-time and open source information, should consider practicing increased Operational Security (OPSEC). With advancements in technology, cybercrime is increasingly becoming an issue for the public as well as SLTT law enforcement and fusion centers. When operating in an online environment, remaining cognizant of the potential consequences of oversharing personal information online while not taking the necessary precautions to protect oneself or an organization has been proved to be detrimental. The guide *Understanding Digital Footprints—Steps to Protect Personal Information*, while directed towards law enforcement, provides material designed to assist in online protection and in not becoming a cyber target and is beneficial knowledge for any individual.³³

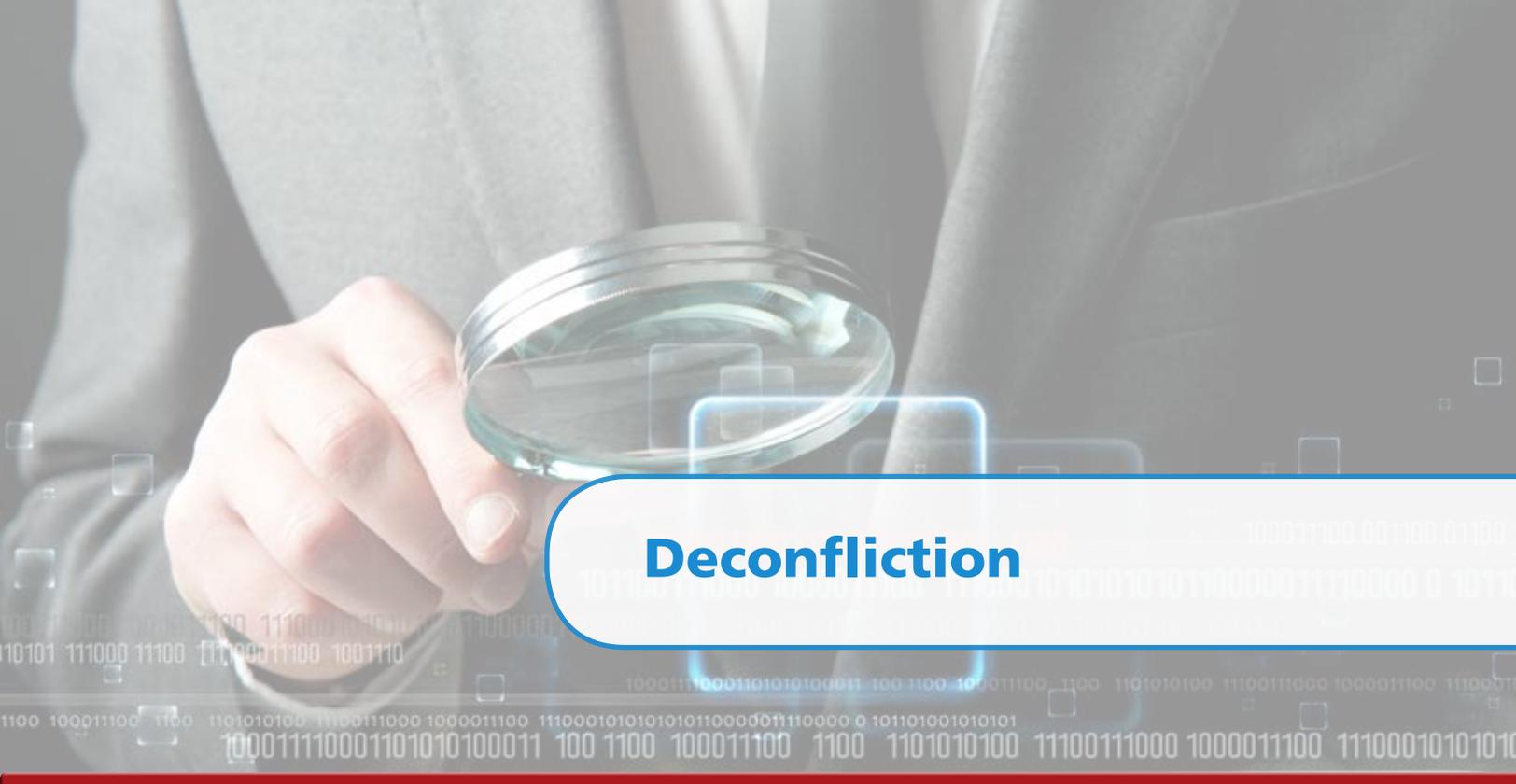


Operational Security Considerations

While there are several methods of maintaining good OPSEC, there are some basic considerations that the guide *Understanding Digital Footprints—Steps to Protect Personal Information* includes:

- ◆ Maintain proper use of the security settings on social media sites to secure profile information.
- ◆ Consider restricting use of location services and “check-in” features on mobile applications.
- ◆ Limiting application and software access to contacts.
- ◆ Create and use strong passwords, change them regularly, and avoid sharing them.
- ◆ Abstain from using identifiable information in passwords or usernames.
- ◆ Connect using secure networks on approved devices and avoid using public WiFi networks for online activity.
- ◆ Enable remote tracking and a wiping feature should a device be lost or stolen.
- ◆ Regularly update systems and programs for improved performance and security.
- ◆ Refrain from sharing too many personal details or identifiable photos on social media and other sites.
- ◆ When not using a device, consider disconnecting from the Internet and logging off and turning it off.
- ◆ Avoid opening unexpected or unknown e-mails, links, and attachments.





Deconfliction

Deconfliction is the process used by law enforcement and intelligence agencies to identify whether or not more than one agency is investigating the same subject, group of subjects, or criminal organization(s).

Deconfliction is an important part of law enforcement operational and analytic activities. The need to share and deconflict case-related information, such as subject information, is increasingly important given the abundance of data being shared and made available via social media. Further, deconfliction assists in identifying duplication of efforts related to the investigation of criminal suspects and also prevents law enforcement officers from investigating each other and their undercover aliases. The incorporation of deconfliction into ROSA-related efforts will help reduce errant investigations and improve information sharing among law enforcement.

State, local, and federal partners are enhancing the three interconnected nationwide event deconfliction systems—the RISS Officer Safety Event Deconfliction System (RISSafe™), the Secure Automated Fast Event Tracking Network (SAFETNet), and the Washington/Baltimore High Intensity Drug Trafficking Area’s (HIDTA) Case Explorer—which should be used for ROSA-related deconfliction.³⁴ Information searched on via a deconfliction system should

be directly related to a law enforcement investigation. The data should be validated prior to the search to ensure that entry criteria are met, including that the information was legally gathered. Supplemental training on existing shared deconfliction systems to ensure that users are properly entering, sharing, and extracting information is highly recommended. Law enforcement personnel should be knowledgeable of the deconfliction systems used by their agency and their partners and any related policies.

As deconfliction systems are used, law enforcement personnel should be aware that open source information, particularly that which is used as a part of most social media sites, such as screen names, handles, and monikers, is generally specific to an account holder, although it may not be specific to just one individual. This information can be deconflicted for similar information across participating systems, but users must be aware of the limitations on deconfliction searches. In addition, such information can become PII when combined with other information and should be handled appropriately. If subject or organization information is not available, other additional corroborative information (e.g., telephone number, e-mail address, location) should be included in a search.

To learn more about the deconfliction system(s) available in your jurisdiction, visit www.ncirc.gov/deconfliction.

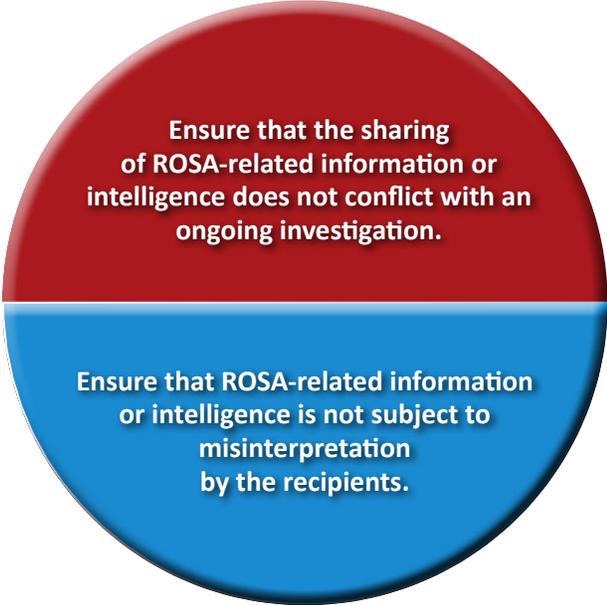


Dissemination of ROSA-Related Information or Intelligence

SLTT law enforcement agencies and fusion centers conducting ROSA as a part of their information-gathering or intelligence development function should establish a dissemination plan to identify procedures for disseminating ROSA-related information or intelligence. A dissemination plan will help limit stakeholders who receive information and intelligence in a manner consistent with need-to-know and right-to-know requirements established by the agency. The dissemination plan should document the appropriate methods for how and when information and intelligence derived through the use of ROSA may be shared and with whom. The dissemination plan should stress the importance of properly handling personally identifiable information (PII) in a manner that protects an individual's privacy, civil rights, and civil liberties. For example, an agency should periodically reevaluate its dissemination lists to ensure that they include the proper recipients and are aligned with the content of the communication.

Dissemination Considerations

When developing a dissemination plan for ROSA-related information and intelligence products, SLTT law enforcement and fusion centers should consider the following:



Ensure that the sharing of ROSA-related information or intelligence does not conflict with an ongoing investigation.

Ensure that ROSA-related information or intelligence is not subject to misinterpretation by the recipients.

Application of the appropriate dissemination caveat when sharing information or intelligence developed with ROSA (Unclassified, For Official Use Only, Law Enforcement Sensitive, etc.) reinforces that only the appropriate partners should receive the information.



Reevaluation of Existing Policies, Procedures, Products, and Resources

SLTT law enforcement, analytic personnel, and partners should consider the frequently changing ROSA environment when reevaluating existing policies, procedures, analytical products, and resources used to conduct ROSA. When law enforcement and analytic personnel reevaluate their agency's ROSA-related policies and procedures, they should consider the following:

Reevaluation of Existing Policies, Procedures, and Tools

Conduct a ROSA evaluation process or an after-action report (AAR) with involved partners to gauge the effectiveness of ROSA at the conclusion of a particular large public event, investigation, emergency response situation, etc.

Consider changes and updates to ROSA tools and how those changes and updates affect the methods, accuracy, effectiveness, and relevancy of the tools when conducting ROSA.

Review changes in P/CRCL laws and regulations and update the appropriate policies to reflect the changes.

Establish the relevancy of intelligence and investigative products containing ROSA and the dissemination methods of that information.

Address and emphasize the need for OPSEC regularly.

Use relevant, updated, and current training mechanisms, such as webinars, information bulletins, analyst-to-analyst exchanges, and local working groups.

Understand outside factors that may shape how and when ROSA can be conducted, such as the changes in the use of technology, exploitation and use of services, and incidents that may elevate the need for ROSA.



ROSA-Related Training

ROSA-related training can be beneficial to law enforcement and analytic personnel with varying levels of knowledge, from a basic understanding of open source analysis, a more in-depth seminar on current tools and techniques, or even a course on cybercrime. Training is critical to understanding open source analysis and how to best use it for investigations and public safety while protecting the P/CRCL of individuals and organizations.

ROSA-related training is available from multiple law enforcement and criminal justice entities and various nongovernmental organizations and can vary in focus. Training courses may cover various open source analysis- and cyber-related topics for law enforcement and analytic personnel, including, but not limited to:

- ◆ The fundamentals of open source information and intelligence
- ◆ Legal requirements (including mission and authorities)
- ◆ P/CRCL protections (including audit, oversight, and accountability)
- ◆ Operational security (e.g., using undercover accounts, methods of obscuration, and methods of nonattribution)



TRAINING

Examples of no-cost training offered by federal partners that focuses on open source analysis include:

- ◆ U.S. Department of Homeland Security's (DHS) Open Source Practitioners' Course (OSINT)
- ◆ National White Collar Crime Center's (NW3C) Social Media Basics³⁵ and Social Media and Technical Skills online³⁶ training
- ◆ U.S. Drug Enforcement Administration's (DEA) Social Media Investigations Course
- ◆ DHS's Privacy, Civil Rights, and Civil Liberties Training³⁷
- ◆ U.S. Secret Service's (USSS) National Computer Forensics Institute³⁸
- ◆ Federal Emergency Management Agency's (FEMA) Social Media in Emergency Management³⁹
- ◆ FBI's Cyber Shield Alliance⁴⁰
- ◆ DHS Cyber Crimes Investigations Training

- ◆ Principles of open source research
- ◆ Search and analytic tools for open source analysis
- ◆ Developing threat assessments
- ◆ Managing data resulting from ROSA
- ◆ Critical thinking to reduce biases
- ◆ Geographic information systems (GIS)
- ◆ Dissemination protocols
- ◆ Retention of information pursuant to privacy and ROSA policies
- ◆ Applicability of 28 CFR Part 23 and its requirements
- ◆ Collection, authentication, and preservation of evidence for investigation and/or trial

Many training programs geared towards analysts and investigators should include a section on ROSA, such as introductory analyst training; however, there are options for training specifically focused on ROSA. Numerous methods exist to educate law enforcement and analytic personnel on current ROSA-related tools, analytic techniques, recommended practices, and training. Although detailed ROSA training may not be critical for all agency personnel, agencies that develop in-house ROSA training for their law enforcement and analytic personnel should address some basic training elements highlighted in this resource.



Recommended Practices for Law Enforcement and Analytic Personnel Using ROSA

- ◆ Have a strong policy in place on conducting ROSA before using open source analysis for investigative or law enforcement intelligence purposes. All policies and procedures must be compliant with the U.S. Constitution, the respective state's constitution, and the applicable laws, rules, and regulations, as appropriate. Involve the privacy officer and legal counsel with the development and review of agency policies related to ROSA.
- ◆ Identify policy, training, and supporting resources that can help address context challenges when social media content is written in a foreign language or makes unfamiliar cultural references.
- ◆ Report violations or suspected violations of the agency policy.
- ◆ Focus only on public safety, criminal activity, and suspicious behavior, rather than on constitutionally protected expression or activities.
- ◆ Limit the collection of publicly available social media information to that which is reasonably related to the purpose of the search.
 - Limit the collection to relevant contacts, connections, and the speech of others.
 - Protected activity may take many forms, and social media platforms shape the message and its meaning. Protected speech can include text, emojis, pictures, videos, music and lyrics, and "Likes," as well as the individual's decision to post, share, respond, or repost.
- ◆ Specify that social media should only be collected without regard to an individual's viewpoint or the fact of speaking itself, unless expressly relevant to the enforcement of a statute or regulation.
- ◆ Receive supervisory approval and oversight before conducting open source analysis.
- ◆ Establish an audit capability for ROSA activities (e.g., prior to conducting ROSA, law enforcement and analytic personnel may provide a supervisor sufficient information to support a ROSA request, and such requests could then be audited on a periodic basis).
- ◆ Retain social media postings in accordance with agency ROSA retention policy.
- ◆ Use only authorized accounts, as appropriate for the matter, to log in to social media sites.
- ◆ Adhere to the agency policy relating to online undercover activity, seeking supervisory approval, documenting the law enforcement or analytic personnel activity, periodically reviewing the activity, and auditing undercover processes and behaviors (including authorization time frames for undercover activities).
- ◆ Actively engage on social media sites only as permitted by agency policy.



Recommended Practices for Law Enforcement and Analytic Personnel Using ROSA (continued)

- ◆ Follow your current policy; do not seek or retain information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.
 - When participating on a Joint Terrorism Task Force (JTTF) or any other federal law enforcement task force or when documenting a suspicious activity report (SAR) or an Information Sharing Environment (ISE) SAR in the Nationwide Suspicious Activity Reporting Initiative (NSI), race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity **must not be considered as factors** creating suspicion. However, those attributes may be documented in specific suspect descriptions for identification purposes or when directly related to participation in an identified criminal activity or enterprise.
- ◆ Do not assume that those who espouse “offensive” views are criminals or will eventually commit a crime, in the absence of specific and articulable facts relevant to potential criminal activity.
- ◆ Use only agency equipment or accounts for official investigative purposes.
- ◆ Always store social media postings in officially approved case files or records management systems (not on unapproved external storage or personal storage drives).
- ◆ Always verify website addresses in social media posts that appear to link to URLs instead of directly clicking on links.
- ◆ Ensure that agency security policies allow for the timely distribution of information and intelligence products to stakeholders.
- ◆ Understand that the capabilities of tools used by the agency may change and how those changes can impact P/CRCL protections, and be vigilant about how and why the agency is using those particular tools.

ENDNOTES

1. <https://it.ojp.gov/GIST/101/National-Criminal-Intelligence-Sharing-Plan>.
2. <https://it.ojp.gov/GIST/150/National-Criminal-Intelligence-Sharing-Plan-Version-2-0>.
3. https://it.ojp.gov/documents/28cfr_part_23.pdf.
4. Not all criminal intelligence products are subject to the operating principles identified in 28 CFR Part 23—only those intelligence products that include “criminal intelligence information” as that term is defined in 28 CFR Part 23. For additional information on criminal intelligence information, see Appendix I and visit <https://28cfr.iir.com>.
5. As identified in the *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities—Guidance and Recommendations*, this guidance focuses on the apparent/overt level of engagement. For an overview of the various levels of engagement, see <https://it.ojp.gov/GIST/132/Developing-a-Policy-on-the-Use-of-Social-Media-in-Intelligence-and-Investigative-Activities--Guidance-and-Recommendations->.
6. For further information about P/CRCL protections, refer to the section on Privacy, Civil Rights, and Civil Liberties Considerations and Appendix III of this guidance.
7. A list of recommended practices for using ROSA is available on page 23.
8. *Virginia v. Black*, [538 U.S. 343, 359 \(2003\)](#).
9. *Id.*
10. See page 9 for P/CRCL considerations regarding true threats and political advocacy.
11. Examples include criminal history records and other fact-based records, criminal intelligence information, and suspicious activity reports (SARs) and terrorism-related SARs (ISE-SARs).
12. See ISE-SAR Functional Standard (Version 1.5.5), https://www.ise.gov/sites/default/files/SAR_FS_1.5.5_IssuedFeb2015.pdf. The authority to conduct ROSA derives from law enforcement’s legal authority to enforce applicable local, state, and federal criminal statutes focusing on the damage to or loss of personal property and threats to personal safety and well-being. The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) is not a source of authority for collecting and using social media.
13. U.S. Constitution Amendment I. (The First Amendment guarantees freedoms concerning religion, expression, assembly, and the right to petition. “It forbids Congress from both promoting one religion over others and also restricting an individual’s religious practices. It guarantees freedom of expression by prohibiting Congress from restricting the press or the rights of individuals to speak freely. It also guarantees the right of citizens to assemble peaceably and to petition their government.”) See https://www.law.cornell.edu/constitution/first_amendment.
14. *Watts v. United States*, 394 U.S. 705 (1969) (per curiam).
15. *Virginia v. Black*, [538 U.S. 343, 359 \(2003\)](#). For an analysis of the communication of threats in interstate commerce under 18 U.S.C. § 875(c), see <https://www.justice.gov/usao/file/851856/download> and *Elonis v. United States*, 135 S.Ct. 2001 (2015). (Holding that the mental state required for a threat under 18 U.S.C. § 875(c) “is satisfied if the defendant transmits a communication for the purpose of issuing a threat, or with knowledge that the communication will be viewed as a threat.”). https://www.supremecourt.gov/opinions/14pdf/13-983_7l48.pdf.
16. *People v. Prisinziano*, 648 N.Y.S.2d 267, 275-76 (N.Y. Crim. Ct. 1996) (citing *Watts*, 394 U.S. at 708).
17. *Watts*, 394 U.S. at 708.
18. *Id.* (In distinguishing a threat from protected speech, the *Watts* Court evaluated the context in which the statement is made, the conditional nature of the statement, and the reaction of the listeners).
19. Note that First Amendment-protected activity may take many forms, including public statements, thoughts, and opinions; association with other people, organizations, and informal groups; religious beliefs, practices, and expressions; and media reporting and news stories. The social media platforms used will also shape the message and its meaning. Protected speech can include text, emojis, pictures, videos, music and lyrics, and “Likes,” as well as the individual’s decision to post, share, respond, and repost. Consider also that content is likely to be found in foreign languages and have cultural references that may be unfamiliar to law enforcement or analytical personnel. Those collecting social media should have access to policy, training, and supporting resources to help address context challenges.

20. Kathleen Ann Ruane, *The Advocacy of Terrorism on the Internet: Freedom of Speech Issues and the Material Support Statutes*, Congressional Research Service (September 8, 2016), <https://fas.org/sgp/crs/terror/R44626.pdf> (citing to *Brandenburg v. Ohio*, 395 U.S. at 448).

21. *Hess v. Indiana*, 414 U.S. 105, 108-09 (1973) (per curiam).

22. See *NAACP v. Claiborne Hardware*, 458 U.S. 886 (1982).

23. See *Virginia v. Black*, 538 U.S. at 362 (citing *R.A.V. v. City of St. Paul*, 505 U.S. at 391).

24. See *People v. Rubin*, 96 Cal. App. 3d 968 (Cal. Ct. App. 1979).

25. *The Advocacy of Terrorism on the Internet: Freedom of Speech Issues and the Material Support Statutes*, Congressional Research Service (2016), at <https://fas.org/sgp/crs/terror/R44626.pdf>.

26. *U.S. v. Williams*, 553 U.S. 285, 299 (2008).

27. *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations* (February 2013), <https://it.ojp.gov/GIST/132/Developing-a-Policy-on-the-Use-of-Social-Media-in-Intelligence-and-Investigative-Activities--Guidance-and-Recommendations->.

28. PII can be defined as one or more pieces of information that, when considered together or in the context of how the information is presented or gathered, are sufficient to specify a unique individual. See Appendix I for ROSA-Related Terms and Definitions.

29. Law enforcement and analytic personnel can avoid overcollection by limiting collection to relevant contacts, connections, and the speech of others.

30. Three examples of policies that address law enforcement's use of open source resources are located in the appendix of the *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities* resource.

- Georgia Bureau of Investigation
- Dunwoody, Georgia, Police Department
- New York City, New York, Police Department

Additional information on the development of law enforcement policies and procedures is located in the Deconfliction section on page 15.

31. For further information on ROSA-related case law and guidance, refer to Appendix II; see also *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations* (addressing

Fourth Amendment privacy law and the Internet and discussing how to document, authenticate, and use open source information for purposes of investigations and trials).

32. *Fusion Center Privacy Policy Development: Privacy, Civil Rights, and Civil Liberties Policy Template*, https://www.it.ojp.gov/documents/d/Fusion_Center_Privacy_Policy_Development_508compliant.pdf. The *Fusion Center Privacy Policy Template* and the *Social Media Guidance and Recommendations* are based upon the Fair Information Practice Principles (FIPPs)—a set of internationally recognized principles that inform information privacy policies within both government and the private sector. Refer to Appendix IV for further information about the FIPPs.

33. *Understanding Digital Footprints: Steps to Protect Personal Information*, Global Advisory Committee (August 2016), <https://www.it.ojp.gov/GIST/1191/File/Understanding%20Digital%20Footprints-09-2016.pdf>.

34. Additional information on event deconfliction is available at <https://www.ncirc.gov/deconfliction/> and in *A Call to Action: Enhancing Officer Safety Through the Use of Event Deconfliction Systems* at <https://it.ojp.gov/gist/149/File/event%20deconfliction%20call%20to%20action0.pdf>.

35. NW3C's Social Media Basics training, <https://www.nw3c.org/training/cybercrime/81>.

36. NW3C's Social Media and Technical Skills training, <https://www.nw3c.org/training/cybercrime/100>.

37. U.S. Department of Justice, Privacy and Civil Liberties, <https://it.ojp.gov/PrivacyLiberty>.

38. USSS National Computer Forensics Institute, <https://www.ncfi.usss.gov/ncfi/index.jsf>.

39. FEMA's Social Media in Emergency Management, <https://training.fema.gov/is/courseoverview.aspx?code=IS-42>.

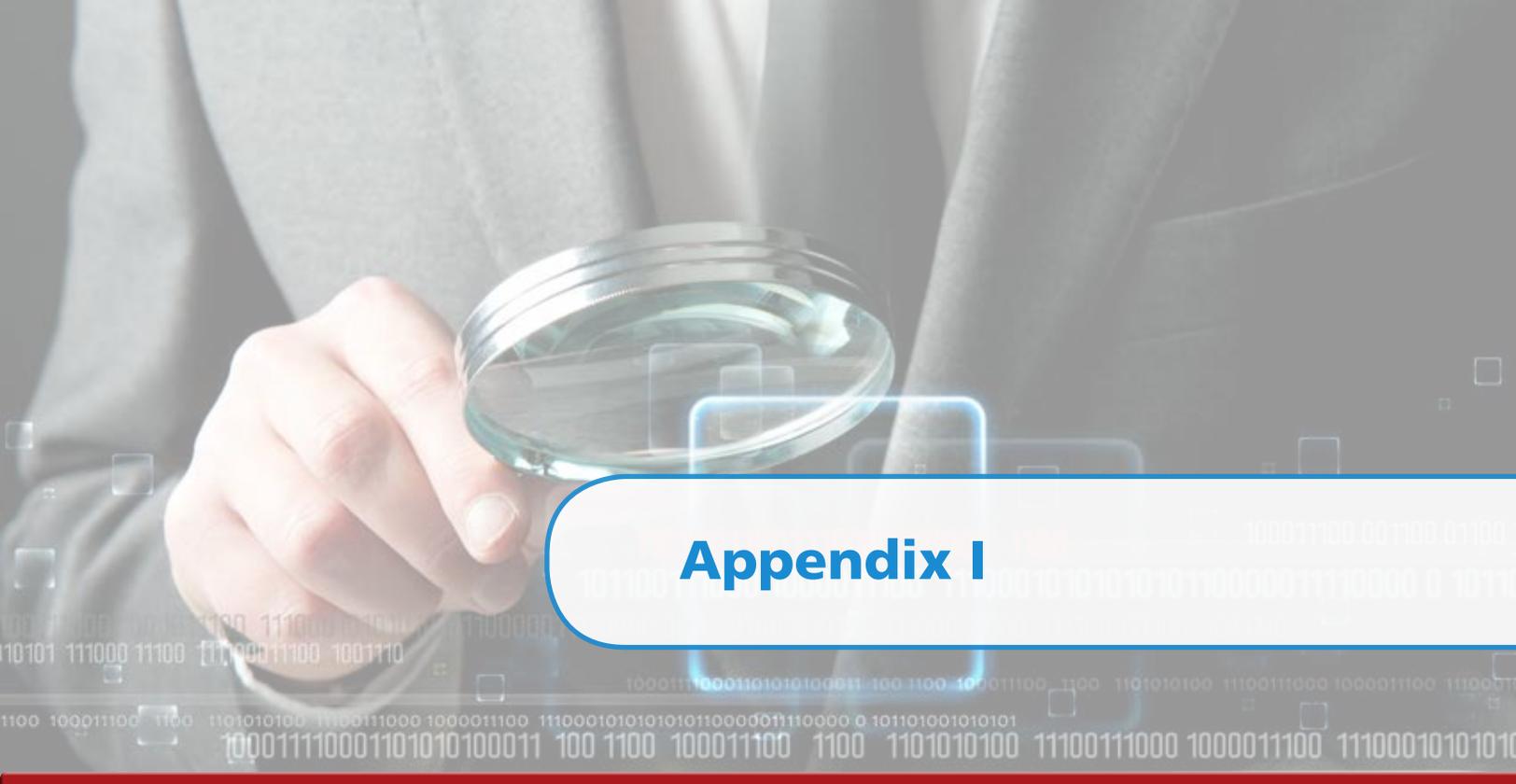
40. FBI's Cyber Shield Alliance is accessible to law enforcement via the Law Enforcement Enterprise Portal (LEEP) at www.cjis.gov as well as the Regional Information Sharing Systems® (RISS) at www.riss.net.

41. 28 Code of Federal Regulations (CFR) Part 23, https://it.ojp.gov/documents/28cfr_part_23.pdf.

42. *National Network of Fusion Centers Final Report*, Glossary, <https://www.dhs.gov/publication/2014-fusion-center-assessment>.

43. *Fusion Center Privacy Policy Development: Privacy, Civil Rights, and Civil Liberties Policy Template* (April 2010), https://www.it.ojp.gov/documents/d/Fusion_Center_Privacy_Policy_Development_508compliant.pdf.

44. Id.
45. *National Criminal Intelligence Sharing Plan*, Version 2.0 (2013), <https://it.ojp.gov/GIST/150/National-Criminal-Intelligence-Sharing-Plan-Version-2-0>.
46. *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations* (February 2013), <https://it.ojp.gov/GIST/132/Developing-a-Policy-on-the-Use-of-Social-Media-in-Intelligence-and-Investigative-Activities--Guidance-and-Recommendations->. See 28 CFR Part 23 in Appendix I.
47. U.S. Department of Homeland Security, “National Infrastructure Protection Plan” (2009), https://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.
48. Nationwide Officer Safety Event Deconfliction website, <https://www.ncirc.gov/deconfliction>.
49. U.S. Department of Homeland Security and U.S. Department of Justice, *Baseline Capabilities for State and Major Urban Area Fusion Centers: A Supplement to the Fusion Center Guidelines* (September 2008).
50. National Fusion Center Association et al., *2014–2017 National Strategy for the National Network of Fusion Centers* (July 2014).
51. Intelligence Community Directive (ICD) 206; Annex A.
52. *Fusion Center Privacy Policy Development: Privacy, Civil Rights, and Civil Liberties Policy Template*, available at https://www.it.ojp.gov/documents/d/Fusion_Center_Privacy_Policy_Development_508compliant.pdf, and *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* (April 2010), available at <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>.
53. *Fusion Center Privacy Policy Development: Privacy, Civil Rights, and Civil Liberties Policy Template*, April 1, 2010, https://www.it.ojp.gov/documents/d/Fusion_Center_Privacy_Policy_Development_508compliant.pdf.
54. Id.
55. The definition for ROSA was developed by the stakeholders who developed this resource guide.
56. *National Network of Fusion Centers Final Report*, Glossary, <https://www.dhs.gov/publication/2014-fusion-center-assessment>.
57. Intelligence Community Directive (ICD) 206; Annex A.
58. *National Network of Fusion Centers Final Report*, Glossary, <https://www.dhs.gov/publication/2014-fusion-center-assessment>.
59. Id.
60. Nationwide Officer Safety Event Deconfliction website, <https://www.ncirc.gov/deconfliction>.
61. *National Network of Fusion Centers Final Report*, Glossary, <https://www.dhs.gov/publication/2014-fusion-center-assessment>.
62. *Virginia v. Black*, 538 U.S. 343, 359 (2003).
63. *National Network of Fusion Centers Final Report*, Glossary, <https://www.dhs.gov/publication/2014-fusion-center-assessment>.
64. *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations* (February 2013), <https://it.ojp.gov/GIST/132/Developing-a-Policy-on-the-Use-of-Social-Media-in-Intelligence-and-Investigative-Activities--Guidance-and-Recommendations->.
65. *Elonis v. United States*, 135 S.Ct. 2001 (2015), Supreme Court of the United States, https://www.supremecourt.gov/opinions/14pdf/13-983_7148.pdf.
66. *Watts v. United States*, 89 S.Ct. 1399 (1969), Supreme Court of the United States, <http://caselaw.findlaw.com/us-supreme-court/394/705.html>.
67. *Brandenburg v. Ohio*, 89 S.Ct. 1827 (1969), Supreme Court of the United States, <http://caselaw.findlaw.com/us-supreme-court/395/444.html>.
68. *Hess v. Indiana*, 94 S.Ct. 326 (1973), Supreme Court of the United States, <http://caselaw.findlaw.com/us-supreme-court/414/105.html>.
69. *NAACP v. Claiborne Hardware Co.*, 102 S.Ct. 3409 (1982), Supreme Court of the United States, <http://caselaw.findlaw.com/us-supreme-court/458/886.html>.
70. *Virginia v. Black*, 123 S.Ct. 1536 (2003), Supreme Court of the United States, <http://caselaw.findlaw.com/us-supreme-court/537/465.html>.
71. *U.S. v. Meregildo*, 883 F.Supp.2nd 523 (S.D.N.Y. 2012), U.S. District Court, Southern District of New York, <http://www.nysd.uscourts.gov/cases/show.php?db=special&id=204>.
72. *U.S. v. Gatson*, 2014 WL 7182275 (D.N.J. Dec. 15, 2014), <https://casetext.com/case/united-states-v-gatson-1>.
73. *Arquiett v. United States*, Case Number 7:13-cv-00752 (N.D.N.Y. 2015), <http://www.law360.com/articles/613340/doj-settles-claims-over-dea-s-fake-facebook-page>.
74. 5 U.S.C. § 552a.
75. 6 U.S.C. § 142.



Appendix I

ROSA-Related Terms and Definitions

28 CFR Part 23—28 Code of Federal Regulations (CFR) Part 23 is a regulation and guideline for law enforcement agencies. It contains implementing standards for operating multijurisdictional criminal intelligence systems receiving federal grant funding. It specifically provides guidance in five primary areas: (1) submission and entry of criminal intelligence information, (2) security, (3) inquiry, (4) dissemination, and (5) the review-and-purge process. This regulation also helps ensure the protection of the P/CRCL of individuals during the collection and exchange of intelligence information.⁴¹

Analysis—An activity whereby meaning, actual or suggested, is derived through organizing and systematically examining diverse information and applying inductive or deductive logic for the purposes of criminal investigation or assessment.⁴²

Analytic Product (may also be called Intelligence Product)—A report or document that contains assessments, forecasts, associations, links, and/or other outputs from the analytic process that may be disseminated for use in the improvement of preparedness postures, risk mitigation, crime prevention, target hardening, or apprehension of offenders, among other

activities. Analytic products may be created or developed jointly with federal, state, and local partners.

Civil Rights—The state has a role in ensuring that all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, gender, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed on government to promote equality. More specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress.⁴³

Civil Liberties—Fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights—the first ten Amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference. Generally, the term “civil rights” involves positive (or affirmative) government action, while the term “civil liberties” involves restrictions on government.⁴⁴

Criminal Intelligence—Information compiled, analyzed, and/or disseminated in an effort to anticipate, prevent, or monitor criminal activity.⁴⁵

Criminal Intelligence Information—Data that has been evaluated and determined to meet criminal intelligence information collection criteria, including that the information is relevant to the identification of or criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in an identified criminal activity or enterprise.⁴⁶

Criminal Nexus—Established when behavior or circumstances are related to an individual's or an organization's involvement or planned involvement in criminal activity or enterprise.

Critical Infrastructure/Key Resources—Critical infrastructure includes systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any federal, state, regional, territorial, or local jurisdiction. Key resources, as defined in the Homeland Security Act, are publicly or privately controlled resources essential to the minimal operations of the economy and government.⁴⁷

Event Deconfliction—The process of determining when law enforcement personnel are conducting an event in close proximity to one another at the same time. Events include law enforcement actions, such as undercover operations, surveillance, and executing search warrants. When certain elements (e.g., time, date, location) are matched between two or more events, a conflict results. Immediate notification is made to the affected agencies or personnel regarding the identified conflict.⁴⁸ *See also—Target Deconfliction*

Fusion Center—A collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity.⁴⁹

National Network of Fusion Centers—The National Network of Fusion Centers is a decentralized, distributed, self-organizing national asset composed of state and major urban area fusion centers and

their respective nodes within each center's area of responsibility (AOR). The function of the National Network is to collaborate across jurisdictions and sectors to effectively and efficiently detect, prevent, investigate, and respond to criminal and terrorist activity.⁵⁰

Open Source Information—Synonymous with publicly available information. It includes traditional and social media information, data, subscription services available for purchase, and other media.⁵¹ *See also—Publicly Available Information and Social Media*

Personally Identifiable Information (PII)—PII refers to one or more pieces of information that, when considered together or in the context of how the information is presented or gathered, are sufficient to specify a unique individual.⁵² Types of PII information can be:

- **Personal characteristics:** Examples include height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, a photographic image, X-rays, and biometrics information, such as fingerprints, DNA, and retinal scans, or template data (e.g., voice signature, facial geometry).
- **A unique set of numbers or characters assigned to a specific individual:** Examples include name, alias, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, information identifying personally owned property (e.g., vehicle registration number or title number), Integrated Automated Fingerprint Identification System [IAFIS] identifier, or booking or detention system number. Cyber-related examples include uniform resource locators (URLs) and Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people.
- **Descriptions of event(s) or points in time:** Examples include information in documents such as police reports, arrest reports, and medical records.
- **Descriptions of location(s) or place(s):** Examples include geographic information systems (GIS)

locations, electronic bracelet monitoring information.

Privacy—Individuals' interests in preventing the inappropriate collection, use, and release of personal information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the capacity to be physically left alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); or to avoid being seen or overheard in particular contexts.⁵³

Publicly Available Information—Any information that any member of the public could lawfully obtain by request or observation (not amounting to physical surveillance) and information, including public communications, that is lawfully accessible to any member of the public. Publicly available covers information that has been published or broadcast for public consumption, is available on request to the public, is accessible online or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is obtained by visiting any place or attending any event that is open to the public, or is made available at a meeting open to the public.⁵⁴ *See also—Open Source Information and Social Media*

Real-Time and Open Source Analysis—The process conducted by law enforcement 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.⁵⁵

Request for Information—A request initiated by the fusion center or a fusion center stakeholder (e.g., law enforcement agency or the U.S. Department of Homeland Security) that could include, but is not limited to, requests for information or intelligence products or services such as name traces, database checks, assessments, subject-matter expertise assistance, or finished intelligence products.⁵⁶

Social Media—User-generated content on a Web-based technology platform that enables people to communicate and share both information and resources through an instantaneous distribution or information that is not necessarily publicly available.⁵⁷ *See also—Open Source Information and Publicly Available Information*

Strategic Analysis—Strategic analytic products include assessments providing an overall picture of the intent and capabilities of specific terrorist or criminal groups, including likely tactics, techniques, and procedures. Strategic analytic products might also include trend analysis and forecasting.⁵⁸

Tactical Analysis—Tactical analytic products assess specific, potential threats related to near-term time frames or major events. They involve issues that need immediate information capabilities to assist decision making on current operations. Tactical cyber analysis includes analysis of cyber indicators, including but not limited to Internet Protocol addresses, domains, hashes, and log files, for the purpose of assisting in case support or operational goals.⁵⁹

Target Deconfliction—Applies to subjects, gangs, locations, telephone numbers, vehicles, and other information about criminal activity. As a part of the total deconfliction process, this information should be deconflicted using appropriate local, state, tribal, regional, and/or federal target deconfliction systems to determine whether there is conflicting activity by other agencies involving the same information. If a conflict is discovered in either target or investigative activity, contact shall be made with the other agency to resolve and coordinate issues and information. Target deconfliction helps increase the ability to link investigations, helps connect suspects and cases, maintains the integrity of investigations, and strengthens information sharing.⁶⁰ *See also—Event Deconfliction*

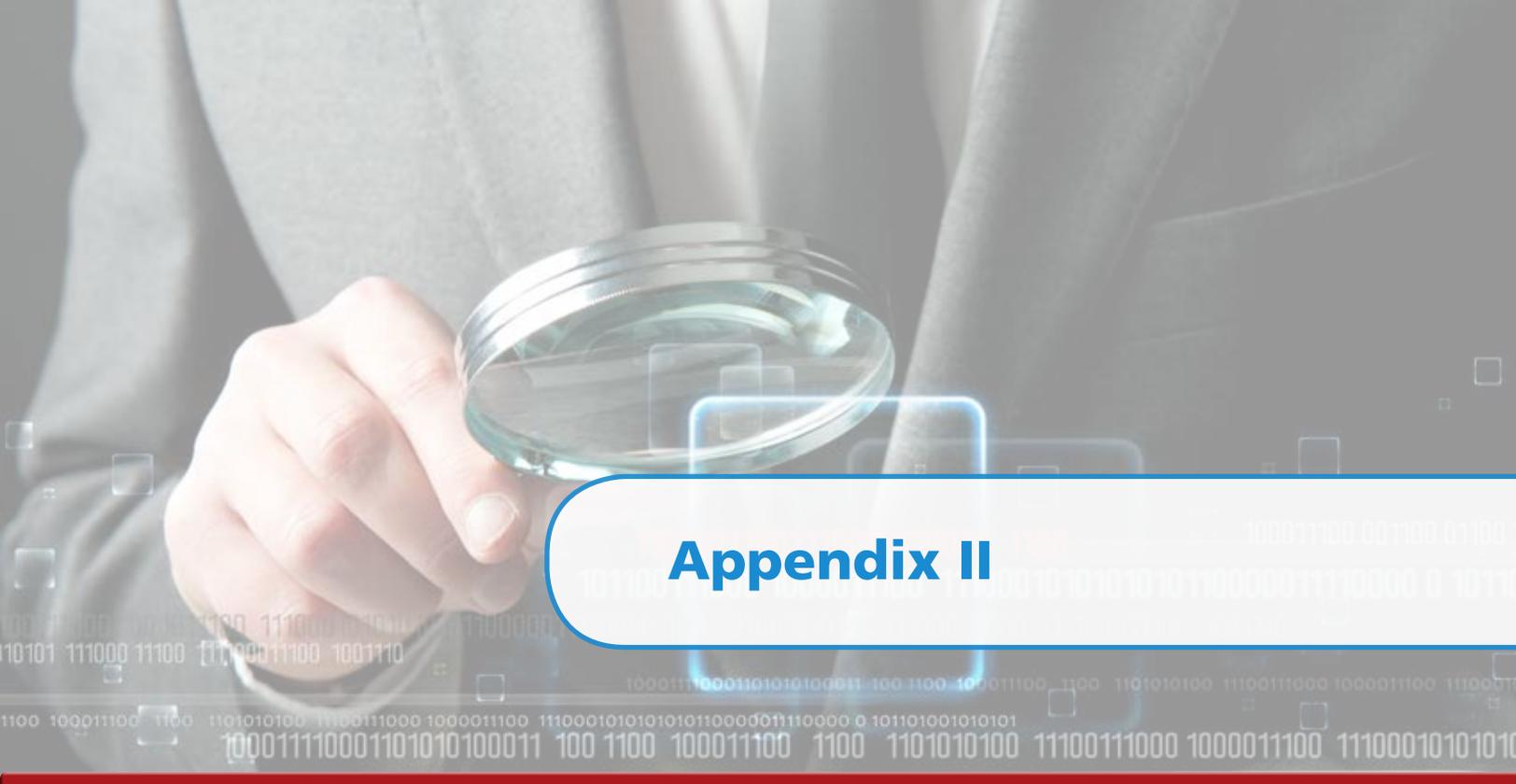
Threat—Natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.⁶¹

True Threats—“[T]hose statements where the speaker means to communicate a serious expression of an intent to commit an act of unlawful violence to a particular individual or group of individuals.” Such threats are

referred to as “true threats” and are not protected by the First Amendment to the U.S. Constitution.⁶²

Tips and Leads—Information provided from fusion center stakeholders, the general public, or other sources regarding potentially criminal activity, including terrorism.⁶³

Valid Law Enforcement Purpose—A purpose for information/intelligence gathering, development, or collection, use, retention, or sharing that furthers the authorized functions and activities of a law enforcement agency, which may include the prevention of crime, ensuring the safety of the public, public and private structures and property, furthering officer safety (including situational awareness), and homeland and national security, while adhering to law and agency policy designed to protect the P/CRCL of Americans.⁶⁴



Appendix II

ROSA-Related Case Law and Guidance

United States Supreme Court decisions are included in this Appendix to assist law enforcement and analytic personnel in distinguishing between criminal conduct (e.g., true threats, incitement of violence) and lawful speech, in a manner that is consistent with the First Amendment to the U.S. Constitution.

Other case law that affects ROSA includes a recent Supreme Court decision, *Elonis v. United States*. This case can serve as a precedent in any court. Lower court cases are also identified below. Although not precedential, these cases can provide some guidance as to how courts may rule in their relevant areas. In addition, a civil case, which may provide some guidance on acceptable law enforcement practices, is discussed in this section. While these cases may provide guidance, this appendix is not a comprehensive list of all cases that may impact ROSA, and it is always important for law enforcement agencies and fusion centers to have legal counsel for their organization examine the cases for alignment with the governing legal authorities in their jurisdiction.

U.S. Supreme Court Cases

Elonis v. United States (2015):⁶⁵ This case dealt with the definition of a threat under 18 U.S.C. § 875(c), which makes it a federal crime to transmit any communication in interstate or foreign commerce containing a threat to injure the person of another. Here, the Supreme Court overturned the defendant's conviction for making threats against his wife, his former employer, and state and federal law enforcement officers on his Facebook page. The Court ruled that the lower court had erred in defining a "threat" as a statement that a reasonable person, in light of the full context, would interpret as a threat without considering the intent of the defendant. Instead, the Court held that "the mental state requirement in Section 875(c) is satisfied if the defendant transmits a communication for the purpose of issuing a threat, or with knowledge that the communication will be viewed as a threat."

Watts v. United States (1969):⁶⁶ This case distinguished a threat from constitutionally protected political rhetoric. Here, the Supreme Court overturned the defendant's conviction for making threats against the life of the President. At a public rally, after having received his draft papers, the defendant publicly declared, "They always holler at us to get an education. And now I have already

received my draft classification at 1-A and I have got to report for my physical this Monday morning. I am not going. If they ever make me carry a rifle, the first man I want to get in my sights is L.B.J.” The Court ruled that the government did not prove a “true threat” in the case. In context, the Court saw no other interpretation other than political hyperbole in front of an antiwar crowd. The Court found that “(t)he language of the political arena, like the language used in labor disputes . . . is often vituperative, abusive, and inexact.”

Brandenburg v. Ohio (1969):⁶⁷ This case found that the Ohio Criminal Syndicalism Act failed to distinguish advocacy from incitement to commit imminent lawless actions and as such was unconstitutional. In the case, a member of the Ku Klux Klan had been convicted of violating the act by advocating for crime and violence as means to further political ends. He also advocated the teaching of criminal syndicalism doctrines. The defendant was sentenced to ten years in prison as a result of the conviction. The Supreme Court overturned the conviction and held that the act could not stand because it punished mere advocacy in violation of the First and Fourteenth Amendments.

Hess v. Indiana (1973):⁶⁸ This case distinguished between “fighting words” and constitutionally protected free speech. The defendant in this case was convicted for disorderly conduct for yelling at an antiwar protest, “We’ll take the [expletive] street later,” while law enforcement attempted to clear the street. Testimony in the case demonstrated that the defendant did not appear to direct his words to any particular person or group and so could not be considered fighting words. Moreover, the Supreme Court found that, in context, the language could (at best) be considered advocacy of violence without any intention of creating “imminent disorder,” and so the defendant’s words could not be considered to have a “tendency” to lead to violence.

NAACP v. Claiborne Hardware Co. (1982):⁶⁹ In this case, the U.S. Supreme Court overturned an injunction against boycotters and ruled on issues of liability related to protests. A local branch of the NAACP initiated a boycott of white merchants in Mississippi in an effort to seek racial justice and equality. Certain merchants filed suit for injunctive relief and damages against the protestors. While the protestors were initially held liable in part for damages by the Mississippi Supreme Court,

the U.S. Supreme Court ultimately found that they could not be held liable for actions protected by the First Amendment. The Court determined that the protests were largely peaceful in nature and that protestors could not be held liable for damages resulting from nonviolent, protected protests. The merchants were entitled only to compensation for damages resulting from illegal actions. Moreover, the Court also found that the language of one protestor in particular, who stated that those who broke the boycott would “have their necks broken,” in context did not incite violence. The Court noted that, in their totality, the speaker’s words commonly sought unification through passionate words and when those words do not incite “imminent lawless action,” the speaker cannot be held liable.

Virginia v. Black (2003):⁷⁰ This case distinguished between the right to display the symbols from one’s ideology from attempts to intimidate others. Two defendants were convicted of attempting to burn a cross with intent to intimidate. The U.S. Supreme Court found that the statute was not unconstitutional on its face but did vacate the judgment in part. The Court noted that cross burning is a “symbol of hate” intertwined with the Ku Klux Klan and that while in and of itself cross burning does not convey a message of intimidation, it could be used in such a manner. However, when used for intimidation purposes, action that would otherwise be constitutionally protected can be considered “true threats” that may be prohibited by the state.

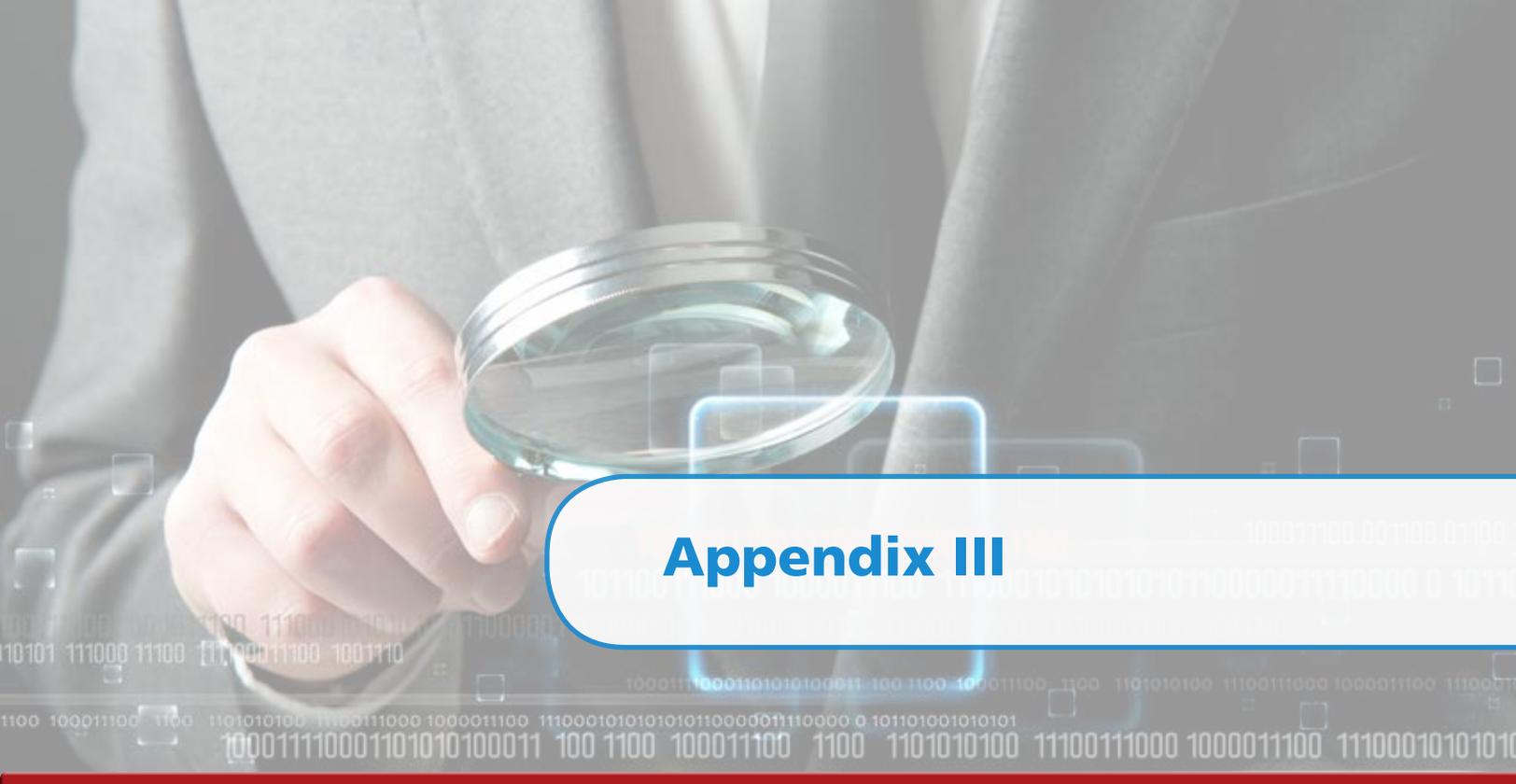
Lower Court Cases

U.S. v. Meregildo (2012):⁷¹ In this case, law enforcement was able to view the defendant’s Facebook profile through the Facebook account of one of the defendant’s “friends” and saw that the defendant’s Facebook profile contained messages regarding prior acts of violence, threats of new violence to rival gang members, and efforts to maintain the loyalties of other alleged members of the defendant’s gang. The U.S. District Court for the Southern District of New York held that this action by law enforcement did not violate the defendant’s Fourth Amendment rights, stating that “where Facebook privacy settings allow viewership of postings by ‘friends,’ the Government may access them through a cooperating witness who is a ‘friend’ without violating the Fourth Amendment.”

U.S. v. Gatson (2014):⁷² In this case, law enforcement was able to view photographs on the defendant's Instagram account by "friending" the defendant. These photos depicted the defendant with large amounts of cash and jewelry and were used as evidence in the defendant's trial for conspiracy to transport and receive stolen property. Here, the U.S. District Court for the District of New Jersey held that this activity by law enforcement did not violate the defendant's Fourth Amendment rights and that no search warrant was required for the "consensual sharing" of these photographs.

Relevant Civil Case

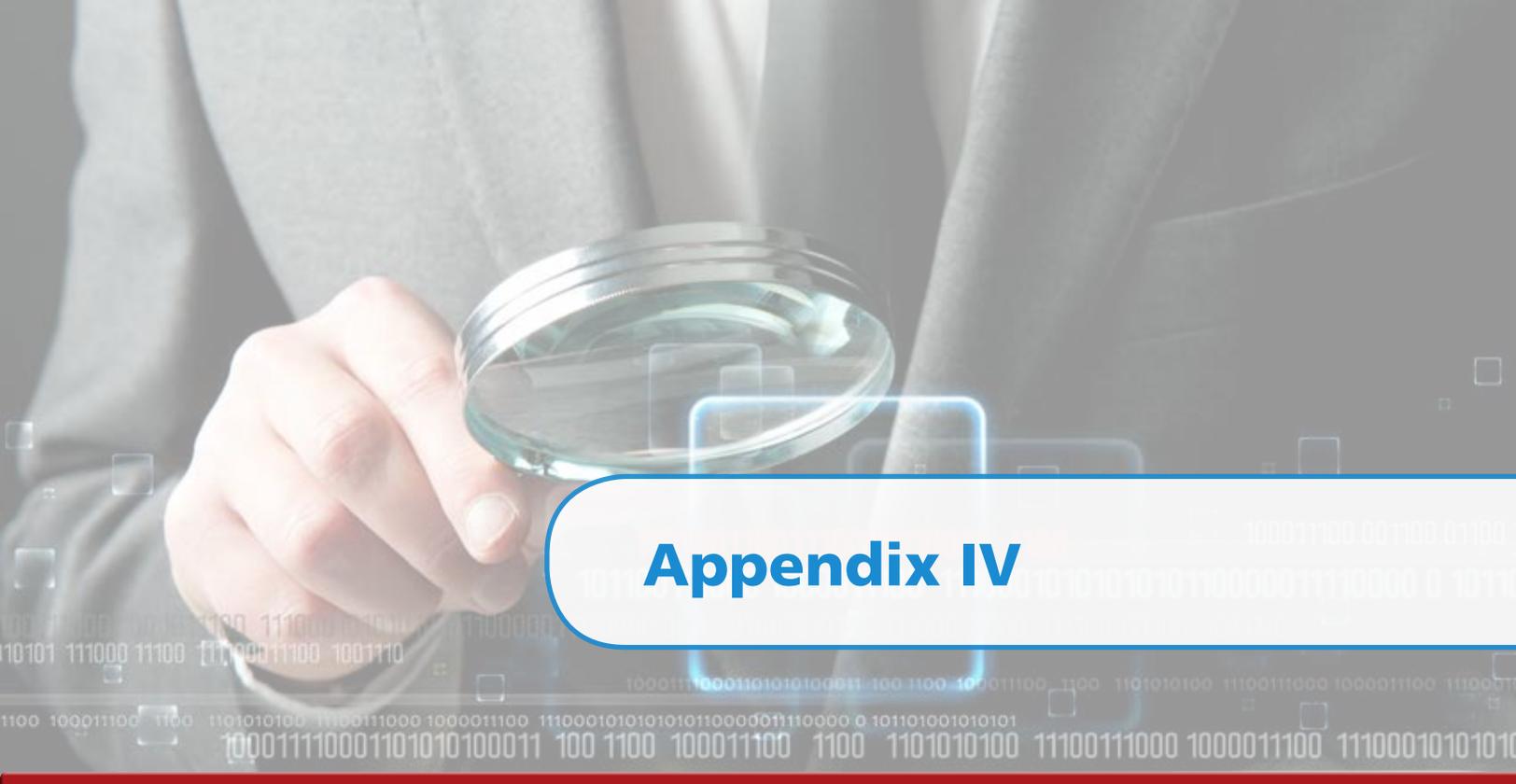
Arquiett v. United States (2015):⁷³ Sondra Arquiett sued the U.S. Drug Enforcement Administration (DEA), claiming that her constitutional rights had been violated after a DEA agent had created a fake Facebook profile posing as her in an attempt to make contact with drug dealers. The plaintiff alleged that a DEA agent lifted photos and other information from her cell phone after she was arrested for cocaine possession with intent to distribute. The DEA reached a \$134,000 settlement with the plaintiff.



Appendix III

ROSA Considerations and Common Practices Related to Personally Identifiable Information (PII)

- ◆ PII collected from ROSA should be governed by agency P/CRCL policy; look for inappropriate handling and consider the potential for harm, inconvenience, unfairness, or embarrassment resulting from inappropriate handling.
- ◆ Be alert to the presence of PII; PII is the primary trigger for the privacy protections in your agency's privacy policy.
- ◆ Review and understand your agency's policy on the collection, use, storage, and dissemination of PII.
- ◆ Evaluate its context of usage to identify and mitigate risks.
 - Understand that as the sensitivity of PII increases, generally so too does the strength of requisite privacy protections.
- ◆ Only gather/collect, use, store, or disseminate PII with a valid law enforcement purpose.
- ◆ Be alert to the possibility that non-identifying information might develop into PII as the analyst or investigator takes certain steps and uses his or her expertise with social media to identify a particular individual.
- ◆ Understand the functionality of common social media platforms regarding a user's ID, username, hashtags, and other possible identifiers.



Appendix IV

Fair Information Practice Principles

The Fair Information Practice Principles (FIPPs) are a set of internationally recognized principles that inform information privacy policies within both government and the private sector.

Although specific articulations of the FIPPs vary and have evolved since their genesis in the 1970s, core elements are consistent among nations, states, and economic sectors. These core elements are incorporated into data privacy laws, policies, and governance documents around the world. For example, the FIPPs are:

- At the core of the Privacy Act of 1974, which applies these principles to U.S. federal agencies.⁷⁴
- Influential internationally, especially as articulated by the Organisation for Economic Co-operation and Development.
- Mirrored in many states' laws and in fusion centers' privacy policies.
- Used by numerous foreign countries and international organizations.

The following formulation of the FIPPs is used and implemented for the Information Sharing Environment (ISE) by the U.S. Department of Homeland Security (DHS).⁷⁵

- 1. Purpose Specification**—Agencies should specifically articulate the authority that permits the collection of personally identifiable information (PII). The purpose(s) for which PII is collected should be specified at the time of data collection. Subsequent use of this data should be limited to the original purpose for which the PII was collected (or other purposes compatible with the original collection purpose).

Implementing the Purpose Specification Principle—Agencies are bound by specific constitutional and statutory authorities that circumscribe their ability to collect PII. The following are examples of ways agencies may implement this principle:

- Ensure that a valid lawful purpose exists and is documented for all collection of PII.
- Include the source and authority for the data so that access restrictions can be applied.
- Upon receipt of data containing PII from third parties, if possible, identify the purpose for which it was collected initially and limit agency use to only those uses compatible with the original purpose supporting collection.
- Ensure that metadata or other tags are associated with the data as it is shared.

- Institute a two-individual review and approval process to consider any Privacy Act or other legal or policy limitation before permitting use or sharing of data for purposes other than that for which it was collected.

2. Data Quality/Integrity—PII collected should be relevant to the purposes identified for its use and should be accurate, complete, and up to date.

Implementing the Data Quality/Integrity Principle—One important way to minimize potential downstream P/CRCL concerns is to ensure that any information collected, stored, and disseminated is accurate. This includes ensuring that the information provides sufficient context for any PII. Possible approaches include:

- Properly labeling PII.
- Determining a policy for safeguarding PII if there are “mixed” databases (i.e., those databases with personal information on U.S. individuals and others, regardless of nationality).
- Instituting a source verification procedure to ensure reporting is based only on authorized data.
- Reconciling and updating PII whenever new relevant information is collected.
- Developing a protocol for ensuring data corrections are passed to those entities with which information has been shared.
- Creating a documented process for identifying and addressing situations in which data has been erroneously received, is inaccurate, or has been expunged.

3. Collection Limitation/Data Minimization—PII should be collected only if the data is directly relevant and necessary to accomplish the specified purpose. PII should be obtained by lawful and fair means and retained only as long as is necessary to fulfill the specified purpose.

Implementing the Collection Limitation/Data Minimization Principle—Collection limitation may be implemented by:

- Designing a data storage system to pull data for review and then, if appropriate, automatically purging data after the specified retention period has been reached.
- Limiting data field elements to only those that are relevant.

- Ensuring that all distributed reports and products contain only that personal information that is relevant and necessary (nothing extraneous or superfluous).
- Ensuring that all shared information with PII meets required thresholds for sharing, such as reasonable suspicion.

4. Use Limitation—PII should not be disclosed, made available, or otherwise used for purposes other than those specified except (a) with the consent of the individual or (b) by the authority of law.

Implementing the Use Limitation Principle—Sharing information should be tempered by adherence to key principles such as “authorized access.” Use limitation may be implemented by:

- Limiting users of data to those with credential-based access.
- Requiring that justifications be entered and logs maintained for all queries with sensitive PII and that an internal review process of those logs takes place at specified intervals.
- Requiring senior analysts to review all reports that use PII before dissemination to ensure that (a) PII is relevant and necessary and (b) the recipient is authorized to receive the information in the performance of an authorized activity.
- Prior to sharing information, verify that partners have a lawful purpose for requesting information.
- Creating multiple use-based distribution lists and restricting distribution to those authorized to receive the information.

5. Security/Safeguards—Agencies should institute reasonable security safeguards to protect PII against loss, unauthorized access, destruction, misuse, modification, or disclosure.

Implementing the Security/Safeguards Principle—This principle can be implemented by:

- Maintaining up-to-date technology for network security.
- Ensuring that access to data systems requires that users meet certain training and/or vetting standards and that such access is documented and auditable.
- Ensuring that physical security measures are in place, such as requiring an identification

card, credentials, and/or passcode for data access; disabling computers' USB ports; and implementing firewalls to prevent access to commercial e-mail or messaging services.

- Implementing a protocol with technical and manual safeguards to ensure the accuracy and completeness of data system purges when records are deleted at the end of their retention period.
- Ensuring that data system purge protocols include complete record deletion on all backup systems.
- Transitioning older repositories into more modern systems to improve access controls.
- Masking data so that it is viewable only to authorized users.
- Maintaining an audit log to record when information is accessed and by whom for review by senior staff at specified intervals.
- Requiring authorized users to sign nondisclosure agreements.

6. Accountability/Audit—Agency personnel and contractors are accountable for complying with measures implementing the FIPPs, for providing training to all employees and contractors who use PII, and for auditing the actual use and storage of PII.

Implementing the Accountability/Audit Principle—Strong policies must not only be in place but also be effectively implemented. Accountability can be demonstrated by:

- Ensuring that upon entry for duty, all staff take an oath to adhere to the privacy and civil liberties protections articulated in the center's or host agency's mission, core values statements, other key documents, and/or the U.S. Constitution.
- Conducting effective orientation and periodic refresher training, including P/CRCL protections, for all individuals handling PII.
- Tailoring training to specific job functions, database access, or data source/storage requirements.
- Conducting regular audits of all systems in which records are kept to ensure compliance with the P/CRCL policies and all legal requirements.
- Following a privacy incident handling procedure for any data breaches or policy violations.
- Denying database access to individuals until they have completed mandatory systems access

training (including training for handling of PII), show a mission need for access, and have any necessary clearances.

- Developing targeted and consistent corrective actions whenever noncompliance is found.

7. Openness/Transparency—To the extent feasible, agencies should be open about developments, practices, and policies with respect to the collection, use, dissemination, and maintenance of PII. Agencies should publish information about policies in this area, including the P/CRCL policy, and contact information for data corrections and complaints.

Implementing the Openness/Transparency Principle—Agencies can implement the Openness/Transparency principle by:

- Providing reports to an internal or external oversight body concerned with P/CRCL issues, including P/CRCL audit results.
- Publishing the P/CRCL policy and redress procedures.
- Meeting with community groups through initiatives or through other opportunities to explain the agency's mission and P/CRCL protections.
- Responding in the fullest way possible to freedom of information and/or sunshine requests and fully explaining any denial of information requests from the public.
- Conducting and publishing Privacy Impact Assessments (PIAs) in advance of implementing any new technologies that affect PII, thereby demonstrating that P/CRCL issues have been considered and addressed.

8. Individual Participation—To the extent practicable, involve the individual in the process of using PII and seek individual consent for the collection, use, dissemination, and maintenance of PII. Agencies should also provide mechanisms for appropriate access, correction, and redress regarding the agency's use of PII.

Implementing the Individual Participation Principle—To the extent appropriate, agencies can implement the Individual Participation principle by:

- Collecting information directly from the individual, to the extent possible and practical.

- Enabling the individual to find out whether an agency maintains a record relating to him or her and, if not (i.e., access and/or correction is denied), then providing the individual with notice as to why the denial was made and how to challenge such a denial.
- Putting in place a mechanism by which an individual is able to prevent information about him or her that was obtained for one purpose from being used for other purposes without his or her knowledge.



Appendix V

Additional Resources

General ROSA-Related Resources

- *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations*, <https://it.ojp.gov/GIST/132/Developing-a-Policy-on-the-Use-of-Social-Media-in-Intelligence-and-Investigative-Activities--Guidance-and-Recommendations->.
- International Association of Chiefs of Police's Center for Social Media, <http://www.iacpsocialmedia.org>.
- National Institute of Standards and Technology, <https://www.nist.gov>.
- Open Source Enterprise, ODNI, <https://www.opensource.gov>.

Protecting Personally Identifiable Information Resources

- *Fusion Center Privacy Policy Development: Privacy, Civil Rights, and Civil Liberties Policy Template*, U.S. Department of Justice's Global Justice Information Sharing Initiative (April 2010), https://it.ojp.gov/documents/d/Fusion_Center_Privacy_Policy_Development_508compliant.pdf.
- National Institute of Standards and Technology's

Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),

<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf>.

- *Understanding Digital Footprints: Steps to Protect Personal Information*, Global Advisory Committee (August 2016), <https://www.it.ojp.gov/GIST/1191/File/Understanding%20Digital%20Footprints-09-2016.pdf>.
- U.S. Department of Homeland Security's (DHS) *How to Safeguard Personally Identifiable Information* factsheet, <https://www.dhs.gov/xlibrary/assets/privacy/privacy-safeguarding-pii-factsheet.pdf>.

P/CRCL-Related Resources

- *Fusion Center Privacy Policy Development: Privacy, Civil Rights, and Civil Liberties Policy Template* (April 2010), https://www.it.ojp.gov/documents/d/Fusion_Center_Privacy_Policy_Development_508compliant.pdf.
- *Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) v. 1.5.5* (February 2015), https://www.ise.gov/sites/default/files/SAR_FS_1.5.5_IssuedFeb2015.pdf.
- *Privacy, Civil Rights, and Civil Liberties Audit*

Guidance for the State, Local, Tribal and Territorial Intelligence Component (September 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>.

- Privacy Line Officer Training, https://www.ncirc.gov/Training_Privacy_LineOfficer.aspx.
- *Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies* (December 2011), <https://it.ojp.gov/documents/d/Recommendations%20for%20First%20Amendment-Protected%20Events%20for%20state%20and%20local%20Law%20Enforcement.pdf>.
- *U.S. Department of Justice, Guidance for Federal Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity* (December 2014), <https://www.justice.gov/sites/default/files/ag/pages/attachments/2014/12/08/use-of-race-policy.pdf>.

- *The Advocacy of Terrorism on the Internet: Freedom of Speech Issues and the Material Support Statutes*, Congressional Research Service, <http://www.fas.org/sgp/crs/terror/R44626.pdf>.

Deconfliction Resource

- National Officer Safety Event Deconfliction website, <https://www.ncirc.gov/deconfliction>.

