Northern California Regional Intelligence Center
Initial Privacy Impact Assessment for
Open Source Social Media Analyses

The Northern California Regional Intelligence Center (NCRIC) is a multi-jurisdiction public safety program created to assist local, state, federal, and tribal public safety agencies and critical infrastructure locations with the collection, analysis, and dissemination of criminal threat information. It is the mission of the NCRIC to protect the citizens of the fifteen Bay Area counties within its area of responsibility from the threat of narcotics trafficking, organized crime, as well as international, domestic, and street terrorism-related activities through information sharing and technical operations support to public safety personnel.

Fundamental to carrying out the NCRIC's responsibilities is doing so in a way that effectively protects the privacy and civil liberties of individuals and the security and confidentiality of sensitive information. To that end, and although not required by law to do so, the NCRIC has developed this initial Privacy Impact Assessment (PIA) for use, analysis, dissemination, retention, and destruction of data derived from the operation of Open Source Social Media tools.

In addition, the NCRIC has initiated development of, and will continue to refine, specific policy and guidelines for the use, analysis, dissemination, retention, and destruction of Open Source Social Media Data at the NCRIC (NCRIC ROSA Policy). To the greatest extent feasible, the NCRIC ROSA Policy will be made publicly available for review and comment.

Scope of this Initial Privacy Impact Assessment

This Privacy Impact Assessment applies to Open Source Social Media Data collected by the NCRIC and NCRIC partner agencies and shared with other regional law enforcement agencies, accessed, and analyzed using software hosted by the NCRIC. It is not intended to apply, and does not apply, to any other types of data accessed or used at the NCRIC or to any collection, use, or handling of any data at individual NCRIC member or contributing entities.

Use and Efficacy of Open Source Social Media Data

Open Source Social Media Technology

Social media platforms are a group of internet-based applications that allow for the creation and exchange of user-generated content. These applications were specifically created for end-users to electronically share information, pictures, videos, experiences, buy and sell products and services, communicate, research, and socialize. These

platforms are accessible by a growing number of devices, including computers, tablets, smart phones, TV's, and gaming consuls. The majority of these platforms are offered at no cost to the end users, relying on advertising fees to generate revenue.

When posting content to most of these platforms, the end-user decides on the accessibility to the content by others. Choices can include making the content available to anyone (the general public), making the content only available to platform users, making the content registered to trusted recipients, or only making the content accessible by the originator.

The vast quantity of Open Source Social Media data requires programs and/or social media search tools (or engines) to efficiently search content. Some of these search capabilities are built into the platform itself. Some search engines are available as separate online applications and are made available for end-users to perform one-time searches, set scheduled searches, create alerts to new content, and store content based on keywords, locations, and/or usernames. There are also subscription (paid) search tools which can include more advance features such as mapping or search capabilities against multiple platforms.

At the NCRIC, such Open Source Social Media Data is accessed and analyzed using social media search tools to enable:

- Identification of threats to public safety or critical infrastructure;
- Creation of alert mechanisms to maintain situational awareness regarding a known threat or public safety hazard;
- Searches of a target location connected to suspected criminal activity.
- Identify criminal activity during major public events.

Adoption and Efficacy of Open Source Social Media Technology

More than 81% of U.S. police agencies surveyed in 2014 indicated that they are using Social Media technology as a tool in investigations.[1] Police agencies around the country have reported notable successes using Social Media technology in thwarting pending crime by stopping an active shooter, mitigating threats toward school students, executing outstanding arrest warrants and actively tracking gang behavior.[2]

[1] LexisNexis® Risk Solutions. (2014). [Survey of Law Enforcement Personnel and Their Use of Social Media]. www.lexisnexis.com/investigations.
[2] *Id.* Page 3.

Privacy and Civil Liberties Implications of Open Source Social Media Data

To date, United States courts and federal and state legal authorities have not found a legitimate expectation of privacy for individuals in Open Source Social Media Data and, as of the date of this initial PIA, no federal or California statutes applicable to the NCRIC or its partner agencies regulate the use of such data. Nonetheless, the NCRIC recognizes that the benefits to public safety of the effective use of Open Source Social Media Data by law enforcement are tempered by the risks posed by inadvertent or intentional misuse of such data to individual privacy and civil liberties, and, more broadly, to the fundamental freedoms that make our society strong.[3]

Potential Individual Privacy and Civil Liberties Harms

Identification of Individuals. Although Open Source Social Media Data, by itself, does not necessarily identify individuals by name or provide other personal information, social media content, including real names, photos, geolocation and associate information can sometimes be used to determine the identity of an individual. If misused, such information could result in harm to individuals, including but not limited to: assumptions about an individual's behavior or associations, personal agendas of individuals accessing the data, or furthering government objectives that are legitimate but beyond the permissible scope for which access to such data was authorized.

Misidentification. Without careful, rigorous, and technically-controlled access and use of Open Source Social Media Data, significant risks of individuals being misidentified as criminal suspects can arise.

Data Quality and Accuracy Issues. Related to misidentification are the challenges of data quality and accuracy. If Open Source Social Media Data associated with individuals and information analyzed along with such data is not kept up to date and accurate, governmental action may be improperly taken against such individuals and unwarranted investigative assumptions may be made.

Non-relevant data. Data regarding a person's location – particularly when collected over an extended period of time – could potentially be misused to infer additional information about an individual that is not relevant to police purposes and potentially sensitive for the individual. Such inferences could include, but are not limited to: non-relevant personal relationships; marital fidelity; religious observance; and political activities. By precisely and proportionally limiting access to Open Source Social Media Data, the risks of such misuse can be reduced and the likelihood of inferring protected/non-relevant character attributions can be minimized.

[3] Such concerns have been reflected in recent judicial and legislative activities. *See, e.g., United States v. Jones* (quoted below); California Senate Bill 1330. A right to privacy is explicitly enshrined in Section 1 of the California Constitution.

These, of course, are not the only potential individual privacy and civil liberties harms from misuse of Open Source Social Media Data. Such potential harms have been widely discussed in recent years, including in the 2009 ALPR Privacy Impact Assessment produced by the International Association of Chiefs of Police, and resources cited therein, and by the American Civil Liberties Union. [4]

Potential Societal Harms

Perhaps of even greater long-term concern than the risks to individual privacy and civil liberties harms discussed above, which are inherent in any governmental access, use, and storage of information about individuals, are the emerging risks to our societal values themselves. The American Civil Liberties Union has warned, for example, that as Open Source Social Media Data becomes accessible to law enforcement, there is a risk to society that the tools open the door for abuses of power and "The way to solve crimes is to go after people who are suspected of specific criminal acts, not spying on the general public".[5]

In a 2014 United States Supreme Court reviewed case (*Elonis v. US*, 13-983 US___ [2015]*)*, Justice Elena Kagan expressed concern about the potential that such a broadly-enforced statute against "threats" made via social media might chill legitimate free speech.[6]

The ACLU and others have expressed concern that Social Media Monitoring systems invade privacy and chill free speech.[7] In support of that position, California Assemblyman Mike Gatto (D-Silver Lake) authored Assembly Bill 1442 (Social Media Privacy) that was signed by Governor Jerry Brown and enacted into law January 1, 2015. This law prohibits the monitoring of school students by school districts without first advising them of the usage of social media monitoring tools and mandating a public comment forum before the administration of a social media monitoring program.[8]

Protecting Privacy and Civil Liberties

---

[4] http://www.theiacp.org/LinkClick.aspx?fileticket=N%2BE2wvY%2F1QU%3D&tabid=87 (This "Privacy impact assessment report for the utilization of license plate readers," published by the International Association of Chiefs of Police, served as a primary information source for this Initial NCRIC PIA) (http://www.aclu.org/blog/tag/license-plate-scanners)

[5] http://www.lowellsun.com/todaysheadlines/ci_27581830/aclu-questions-possible-purchase-online-monitoring-service-by#ixzz3TH0JtEI0."

[6] http://www.csmonitor.com/USA/Justice/2014/1201/Are-Facebook-rants-threats-or-free-speech-Supreme-Court-takes-up-case.-video

[7] https://www.aclusocal.org/ab1442-victory/

[8] http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB1442

The NCRIC ROSA Policy, and the deployment of access control, auditing, revisioning, and data correction and purging technologies, applied to the privacy and civil liberties concerns articulated herein, will provide increased protection for data currency and accuracy, thereby helping to mitigate risks of misidentification, misuse of non-relevant information, and poor data quality. Concepts of proportionality, authorized use, accountability, and other policy and technical controls, will be incorporated, to deter, detect, and control against misuse of Open Source Social Media Data reasonably likely to implicate these types of societal concerns.

Privacy and Civil Liberties Protections for NCRIC Open Source Social Media Data

Although extensive privacy policies already are in place, the NCRIC recognizes that Open Source Social Media Data has unique attributes that must be addressed through additional measures.

From its inception, the NCRIC has taken the issue of privacy and civil liberties seriously. To that end, the NCRIC follows the Information Privacy Policy adopted by the California State Threat Assessment System (STAS Privacy Policy), which includes one State Fusion Center, four Regional Threat Assessment Centers and one Major Urban Area Fusion Center. The STAS Privacy Policy was developed primarily to address the use and handling of criminal intelligence and related information as governed by 28 C.F.R. Part 23, the California Attorney General's Model Standards and Procedures for Maintaining Criminal Intelligence Files, and other applicable legal authorities.

To the extent individual elements of the STAS Privacy Policy are applicable to Open Source Social Media Data, the NCRIC will adapt these elements to its handling of such data.

The NCRIC recognizes, however, that the use of Open Source Social Media and other locational data may, in some cases, present privacy and civil liberties challenges and protective requirements different from those addressed in the STAS Privacy Policy and, as appropriate, the NCRIC will develop and implement additional protections. In addition, the NCRIC will adapt, to the extent reasonably feasible, the Fair Information Principles described in the STAS Privacy Policy to the handling of Open Source Social Media Data. These principles include:

1. Collection Limitation;
2. Data Quality;
3. Purpose Specification;
4. Use Limitation;
5. Security Safeguards;
6. Openness;
7. Individual Participation; and

8. Accountability

Compliance with Applicable Law

As a threshold matter, and as mandated by the STAS Privacy Policy, the NCRIC, and all assigned or detailed personnel, including personnel providing information technology services, private contractors, and other authorized participants in the NCRIC or any other STAS Component, shall comply with all applicable laws protecting privacy, civil rights, and civil liberties.

Use for Authorized Law Enforcement and Public Safety Purposes Only

Open Source Social Media Data will be used only for authorized law enforcement and public safety purposes. Approved users are authorized to access Open Source Social Media Data to:

- Locate individuals subject to arrest or otherwise lawfully sought by law enforcement;
- Locate missing or wanted persons sought by law enforcement;
- Locate witnesses of a criminal investigation;
- Locate missing or stolen goods;
- Support local, state, federal, and tribal public safety department in the identification of targets of ongoing criminal investigations;
- Provide information to organizers and public safety officials during public events to insure the safety of the public
- Protect critical infrastructure sites.

Consistent with the NCRIC ROSA Policy to be further developed over the coming months, information sharing, access control, and use control technology will be utilized to: (1) record and audit the authorized use for which Open Source Social Media Data is being accessed or used in each instance; and (2) incorporate measures designed to prevent attempted access or use of Open Source Social Media Data for non-authorized purposes.

Collection of Open Source Social Media Data

NCRIC receives Open Source Social Media Data from its partner entities, but also utilizes a number of Open Source media search tools to collect data that is within public view, but may not be used for the sole purpose of monitoring individual activities protected by the First Amendment to the United States Constitution.

Examples of Social Media Tools:
Purchasable – Blue Jay, Media Sonar, Geofeedia, EchoSec, Babel Street, Digital Stakeout

Free- EchoSec, TweetDeck, Hootsuite, Advanced Twitter Search, Social Mention, Social Searcher, TwitterFall, Topsy

Dissemination, Secondary Uses, and Commercial/Private Entity Data Sharing

NCRIC Open Source Social Media Data will be disseminated only to authorized law enforcement or public safety officials with proper authority, and for authorized purposes. The NCRIC ROSA Policy will incorporate controls on secondary uses of Open Source Social Media Data. Information sharing, access control, and use control technology will be utilized to enforce and audit these requirements.

Open Source Social Media Data may be shared with owners or operators of critical infrastructure locations in circumstances where reasonable evidence suggests the location is the target of a terrorist attack or other criminal activity.

Except as noted above with regard to critical infrastructure, the NCRIC will not share Open Source Social Media Data with commercial or other private entities or individuals.

Safeguarding and Protecting Open Source Social Media Data

The NCRIC will take all reasonable physical, technological, administrative, procedural, and personnel measures to protect the confidentiality and integrity of Open Source Social Media Data, whether in storage or in transit.

Data Quality and Accuracy

The NCRIC will take all reasonable measures to ensure that Open Source Social Media Data is accurate and up-to-date. When errors are discovered, corrections will be made promptly and reasonable efforts will be taken to identify, locate, and update information that has been shared with other entities pursuant to the dissemination policy.

Data Vetting and Decision Making

The NCRIC ROSA Policy will establish policies and guidelines requiring human evaluation and verification in determining the relevance of Open Source Social Media Data to an active investigation or other authorized law enforcement or public safety effort. To the greatest extent feasible, open source social media data utilized in investigations will be corroborated by other information prior to using such data as the basis for subsequent law enforcement action.

Data Retention and Destruction

While continuing to refine its ROSA Policy, the NCRIC will incorporate reasonably feasible procedural and technological measures to enforce data retention and destruction requirements imposed by the originators of data received and electronically stored by the NCRIC. The NCRIC will collect and analyze empirical data to support an evaluation of reasonable retention standards for Open Source Social Media Data. During this period of analysis, the NCRIC will adopt a default, system-wide, one-year retention standard under which Open Source Social Media Data will be purged. Under these standards, if such data does not meet established retention requirements based on relevance to an ongoing criminal investigation (for which other retention standards may apply), it will be removed entirely from NCRIC databases.

Utilizing data gathered over the next year to evaluate the use and efficacy of Open Source Social Media Data, and based on consultations with privacy and civil liberties experts, the NCRIC will continue to develop and refine specific Open Source Social Media Data retention and destruction policies, with additional restrictions applied based upon the intended authorized use. For example, further restrictions on temporal, geospatial, relational, and other factors may be implemented.

Utilizing guidance from the California State Legislature, the passage of AB1442 (Social Media Privacy) calls for the school districts who utilize social media monitoring tools to "(3) (A) Destroy information gathered from social media and maintained in its records within one year after a pupil turns 18 years of age or within one year after the pupil is no longer enrolled in the school district, county office of education, or charter school, whichever occurs first."[9]

Training Obligations of NCRIC Personnel

All personnel with access to NCRIC Open Source Social Media Data will be provided with appropriate training, including privacy and security training.

Auditing and Accountability

All NCRIC personnel with access to Open Source Social Media Data will be responsible for strict compliance with the NCRIC ROSA Policy, and all other applicable legal, regulatory, and policy requirements. The NCRIC will employ auditing technologies to enable tracking of, and accountability for, individual NCRIC participant actions to access, use, disseminate, retain, and/or destroy Open Source Social Media Data. Violations of applicable requirements will result in appropriate disciplinary action, including, if appropriate, denial of additional access to NCRIC facilities and data.

[9] http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB1442

Updates and Revisions to the NCRIC Open Source Social Media PIA

This is an initial Privacy Impact Assessment only. It will be reviewed, and updated as necessary, no less frequently than every 12 months, or more frequently based on changes in data sources, technology, data use and/or sharing, and other relevant considerations. Additionally, updates to this Privacy Impact Assessment may be used to inform continued refinements to the NCRIC ROSA Policy.