RIT | College of Liberal Arts
Center for Public Safety Initiatives

Social Media Intelligence Best Practices

Working Paper 2023-10

Jason Scott, Ph.D.,
Associate Professor, Department of Criminal Justice
Rochester Institute of Technology
jxsgcj@rit.edu

Chloe Sitton,
Research Assistant, Center for Public Safety Initiatives
cls8742@rit.edu

Introduction

This is the second paper in the series that examines the link between social media and retaliatory violence. The first paper (Social Media's Impact on Crime and Retaliatory Violence) provided literature review on this topic. This paper focuses on social media intelligence best practices for law enforcement.

Best Practices

1. Police Departments should distinguish between social media intelligence that relies on the searching and scanning of information available in the public domain versus the collection of information through the covert engagement with individuals through law enforcement created aliases, social media '*dummy*' accounts, or '*fake friending*' (USDOJ & PERF, 2013, p. 13-14). Some local and federal law enforcement agencies (e.g., the Federal Bureau of Investigation) have referred to this later use of social media intelligence as *Social Media Exploitation* (SOMEX)[1]. If incorporating SOMEX, law enforcement agencies should develop clear authorization protocols for the use of undercover aliases/profiles and the covert engagement with suspects and persons of interest (Global Justice Information Sharing Initiative, 2013, p. 14-15). The use of these covert intelligence gathering practices should be addressed and integrated into existing department policy regarding surveillance

[1] The use of SOMEX teams within law enforcement is controversial for a number of reasons. Some SOMEX teams have utilized or "commandeered" the real social media profile identities of confidential informants. Further, the use of these "dummy" accounts represents a violation of the use policies of most social media platforms and has legal ramifications.
https://theintercept.com/2022/05/20/chicago-police-fbi-social-media-surveillance-fake/
https://www.theguardian.com/world/2021/nov/18/facebook-lapd-social-media-surveillance-fake-accounts

operations.

2. Police Departments should proactively use social media intelligence and public domain searches to identify and intervene in potentially violent events like disruptive house parties, violent flash mobs, premeditated gang altercations, terrorist activities, organized hate crimes, etc. This depends on the regular scanning of individuals, groups, and social networks already known to law enforcement. (USDOJ & PERF, 2013, p. 17-22).

3. Police Departments should develop protocols for the evaluation and authentication of evidence obtained through social media intelligence. This includes attention to source reliability and content validation. "…a video posted on YouTube shows individuals allegedly robbing a convenience store; law enforcement personnel should obtain a subpoena to determine what IP address was used to upload the video and identify whom the IP address is registered. Information obtained from social media sites can be a valuable tool; however, comprehensive evaluation and authentication are crucial to ensure the reliability and validity of the information and ensure proper caveats are included, as necessary." (Global Justice Information Sharing Initiative, 2013, p. 15).

4. Police Departments should consider the utilization of available third-party social media exploitation software for scanning public open-source data and the dark web and to assist in organizing evidence obtained from social media and open source intelligence. Examples include Fivecast, Maltego, Penlink, and Skopenow (IALEIA, 2022, p. 12-14). Police Departments should develop training and policy addressing the secure storage, access, and dissemination of data collected by third-party software consistent with already

established internal rules and regulations governing records management and computer/software use. Policy guiding the use of third-party social media exploitation software should address the use of fake social media profile add-on features and determine whether the activation of these optional features is consistent with department policies (see the discussion of SOMEX above).

5. Police Departments should engage community partners with social media intelligence. Community partners can assist law enforcement as content or domain experts. Community-based domain experts can assist law enforcement by providing critical insight and meaning around specific language, hashtags, Emojis, location references, and gang knowledge embedded in social media (see Frey et al, 2020). Additionally, community partners can serve as credible messengers in an effort to intervene and de-escalate situations of retaliatory violence or potential violence based on actionable social media intelligence (see Lane & Stuart, 2020).

6. Most Police Departments have developed policies that provide clear guidance and expectations for the use of social media by their members and employees. However, similar policy that offers clarity and transparency about how social media intelligence is collected, maintained, and used by law enforcement should be developed. Law enforcement should provide appropriate transparency about social media intelligence to enhance public understanding, be proactive and clear in making information publicly available through authorized channels, and protect information about intelligence sources, methods, and activities from unauthorized disclosure. This can help ensure public trust and serves to hold law enforcement accountable for the responsible use of social media

intelligence (Director of National Intelligence, 2015).

References

Director of National Intelligence. (2015, October 27). *Principles of intelligence transparency implementation plan* [PDF]. https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Principles%20of%20Intelligence%20Transparency%20Implementation%20Plan.pdf

Frey, W. R., Patton, D. U., Gaskell, M. B., & McGregor, K. A. (2020). *Artificial intelligence and inclusion:* Formerly gang-involved youth as domain experts for analyzing unstructured Twitter data. *Social Science Computer Review*, 38(1), 42-56. https://doi.org/10.1177/0894439318788314

Global Justice Information Sharing Initiative (2013). *Developing a policy on the use of social media in intelligence and investigative activities: Guidance and recommendations.* https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/developing_a_policy_on_the_use_of_social_media_in_intelligence_and_inves.pdf

International Association of Law Enforcement Intelligence Analysts, Inc. (2022). *Social media awareness for enforcement*. https://www.ialeia.org/docs/Social_Media_Awareness_Enforcement.pdf

Lane, J. & Stuart, F. (2022). How social media use mitigates urban violence: Communication visibility and third-party intervention processes in digital urban contexts. *Qualitative Sociology*, 45, 457-475. https://doi.org/10.1007/s11133-022-09510-w

U.S. Department of Justice, Office of Community Oriented Policing Services & Police Executive Research Forum (2013). *Social media and tactical considerations for law enforcement*. https://portal.cops.usdoj.gov/resourcecenter/RIC/Publications/cops-p261-pub.pdf

About the Center for Public Safety Initiatives

The Center for Public Safety Initiatives is a unique collaboration between RIT's **Department of Criminal Justice**, the City of Rochester, and the criminal justice agencies of Greater Rochester including the Rochester Police Department and Monroe County Crime Lab. Its purpose is to contribute to criminal justice strategy through research, policy analysis and evaluation. Its educational goals include training graduate and undergraduate students in strategic planning and policy analysis.

The foundation of the Center is the practice of action research in which relevant data and analyses are brought to bear on the day to day decision-making processes of organizations. The Center serves the practice of policy development and implementation in real-time.

To access our full library of white papers, visit our website at rit.edu/center-public-safety.

Learn more

- rit.edu/center-public-safety
- CPSI@rit.edu
- (585) 475-6386

This project was supported by Grant No. 2021-15PBJA-21-GG-03050-GUNP awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.