SOCIAL MEDIA AND CRIME ANALYSIS: THE INTERSECTION OF ONLINE POSTING AND LAW ENFORCEMENT INVESTIGATIONS

by

Kevin P. Lopez

A Thesis Submitted to the Faculty of

College of Social Work and Criminal Justice

In Partial Fulfillment of the Requirements for the Degree of

Master of Science

Florida Atlantic University

Boca Raton Florida

December 2023

SOCIAL MEDIA AND CRIME ANALYSIS: THE INTERSECTION OF ONLINE POSTING AND LAW ENFORCEMENT INVESTIGATIONS

by

Kevin P. Lopez

This thesis was prepared under the direction of the candidate's thesis advisor, Dr. Lisa M. Dario, Department of Criminology and Criminal Justice, and has been approved by all members of the supervisory committee. It was submitted to the faculty of the College of Social Work and Criminal Justice and was accepted in partial fulfillment of the requirements for the degree of Master of Science.

SUPERVISORY COMMITTEE:

Lisa M. Dario, Ph.D.
Thesis Advisor

Gabriel T Cesar

Gabriel Cesar, Ph.D.

Diana Sun
Diana Sun (Nov 22, 2023 13:36 EST)

Diana Sun, Ph.D.

Cassandra Atkin-Plunk (Nov 22, 2023 13:49 EST)

Cassandra A. Atkin-Plunk, Ph.D.
Interim Director, College of Social Work
and Criminal Justice

Naelys Luna
Naelys Luna (Nov 30, 2023 09:18 EST)

Naelys Luna, Ph.D.
Dean, College of Social Work
and Criminal Justice

Robert W. Stackman Jr., Ph.D.
Dean, Graduate College

November 30, 2023
Date

ACKNOWLEDGEMENTS

The completion of this thesis would not have been possible without the continued guidance and support of Dr. Lisa M. Dario, Ph. D., who has continued to foster and encourage my interests in academia and the field of criminal justice. Thank you for your unwavering support and for inspiring me to pursue a level of education I never anticipated for myself. Additionally, I would like to express special thanks to all the members of my committee, Dr. Gabriel Cesar, Ph. D., and Dr. Diana Sun, Ph. D., for their continued wisdom, knowledge, and support. Thank you to Florida Atlantic University, for providing the resources necessary to achieve this goal.

I would also like to personally thank my family for their relentless support and encouragement throughout this process. Mikalya McSweeney, Ashley, and Rocket thank you all for being my inspiration.

ABSTRACT

Author:	Kevin P. Lopez
Title:	Social Media and Crime Analysis: The Intersection of Online Posting and Law Enforcement Investigations
Institution:	Florida Atlantic University
Thesis Advisor:	Dr. Lisa M. Dario
Degree:	Master of Science
Year:	2023

The current use of social media platforms has expanded to wider audiences, including police departments and other law enforcement agencies. The vast material being posted online may lead to it being used by police departments due to social media information being open-sourced. The following study will investigate the police's use of social media data by collecting qualitative data from crime analysts through the International Association of Crime Analysts (IACA). Participants completed an open-ended survey describing their experience with collecting data from online social media sources and how it is used to assist with police activity. The results have implications for future research, such as further exploring the methods by which police are expanding their data collection. Caution may be required when sharing information online. Results from the study may inspire future research regarding the privacy and ethical considerations of using social media data collected from the public.

SOCIAL MEDIA AND CRIME ANALYSIS: THE INTERSECTION OF ONLINE POSTING AND LAW ENFORCEMENT INVESTIGATIONS

LIST OF TABLES

LIST OF FIGURES

INTRODUCTION

Police departments in the United States have capitalized on the popularity of social media sites by using information provided by civilians online as data and evidence in criminal investigations. In addition to functioning as a tool for community interactions and communication, social media platforms also act as a space for open-source information and user-generated content to prosper. The more data that is shared online, the more this information can be monitored and 'listened to' for potential illicit and illegal activity (Bartlett et al., 2013; also see Farley & Pierotte, 2017). Social media platforms create online spaces where crimes can be committed, discussed, and investigated. However, the extent to which this information is gathered, analyzed, and implemented into police practices remains limited in knowledge.

As police and law enforcement continue to operate and expand into new online spaces and social media platforms, implementing proper guidelines and ethics becomes increasingly important (Bartlett et al., 2013) to uphold police legitimacy and public trust. The legality of using information collected from social media platforms has yet to be significantly evaluated by the courts in the United States (Melekain & Wexler, 2013). It may still be subject to legal issues. During the expansion of this form of digital investigation, police and law enforcement need to consider their roles and activities online, applying the same considerations used when operating in person. Police activity is increasingly becoming the subject of monitoring by the public, and recordings are easily shared with a broad audience due to the proliferation of social media platforms (Fox &

Rose, 2014; Walsh & O'Connor, 2019) and the accessibility of digital media capturing the public while they interact with law enforcement personnel. The same oversight applied to the police in a public setting needs to be applied to the online spaces that police operate in.

Police departments and other law enforcement agencies have expanded into online spaces and created official social media accounts, which are used to establish a presence online, communicate with the public, and build online relationships with the areas they service (Brainard & Edlins, 2015). Ninety-six percent of American police departments were reported to have adopted official social media accounts, most notably using Facebook, YouTube, and Twitter (Brainard & Edlins, 2015; Hu et al., 2018). Agencies may share or post information online about traffic updates, general notifications, or serious criminal events (Boateng & Chenane, 2020). Social media engagement and dialogue between the community and local police departments can be a way to demystify and humanize the police (Wood, 2020). In times of crisis and uncertainty, the police use these platforms to broadcast information to the public. For example, the Boston Police Department used Twitter to provide live updates during and after the 2013 Marathon bombings to ease the community's concerns and curb the rising spread of misinformation and speculation (Boateng & Chenane, 2020).

There is a knowledge gap in the research surrounding how police departments may use social media to assist in the criminal investigation process and how this intelligence may be used in current applications within police agencies. Additionally, the staff within police departments that gather and use information from online sources will be examined in the current study. Further, what type of information is deemed viable and

how that data can assist agencies is still being determined. As the conversation around data privacy and social media transparency continues, understanding how police agencies collect and use open-source, public information and private data is necessary to ensure that law enforcement agencies maintain public trust and legitimacy. The current study will survey crime analysts' experiences via predominantly open-ended questions. The qualitative responses provided by participants may provide insight into how information and data are gathered from social media sites, how it is analyzed into intelligence, and how that intelligence may be used to assist crime events and criminal investigations.

LITERATURE REVIEW

Public Broadcasting

Social media has allowed police departments to directly communicate with local communities without needing information delivered through a third party (Schneider, 2016). Most police departments use Facebook and Twitter to engage with their communities through plain text posts, photos, and videos (Williams et al., 2018). Williams and colleagues (2018) surveyed 500 police departments regarding their use of social media platforms and found that 95.4% and 66.4% of departments used Facebook and Twitter to share information, respectively.

Social media can notify the public about community safety concerns, including potential criminal issues (Williams et al., 2018). A notable example of rapid communication with the public came in the aftermath of the bombings during the Boston Marathon in 2013. In the uncertainty that followed the bombings, the Boston Police Department (BPD) used Twitter to respond to and speak with the public effectively. The department tweeted information to ease the public's concerns over the situation and prevent further panic. They accomplished this by posting updates regarding the status of the criminal investigation and by correcting floating misinformation (Davis et al., 2014). In the aftermath of the bombings, independent efforts began to gain traction, which started a significant investigation from the public. These speculations were later debunked and determined to be false by the BPD, who used Twitter to correct the misinformation and stop the potential harm it could cause (Davis et al., 2014).

In addition to the more serious notifications, general notifications are commonly shared online. Estimations reveal that more than half of communications from the police online are related to general announcements rather than crime stopping (Williams et al., 2018). A significant amount (74.7%) of online activity is related to pushing information out to the public (Hu et al., 2018). The Oxford Police Department (OPD) in Mississippi has six primary areas of communication shared by the department's official Twitter account, including crimes and arrests, reports of criminal incidents, information and vehicle accidents, police programs and events, missing people or animals, and miscellaneous information (Boateng & Chenane, 2020). The OPD mostly shared information on vehicle accidents (62.29%) and rarely shared information related to crime and disorder (0.45%; Boateng & Chenane, 2020).

For example, police legitimacy in offline capacities already faces difficulties. If they were to transition into online activities, there may be an initial sense of skepticism (Dekker et al., 2020). Police departments may also want to engage less in an official online capacity due to the potential harm it could cause to their image (Dekker et al., 2020). However, communicating differently from their traditional messaging may create an informal sense of legitimacy. To overcome some of these language barriers online while still maintaining a sense of legitimacy and authority, the authors (Dekker et al., 2020) propose the experimentation of different online communication methods, encouraging variability in the delivery of public messages. This is further supported by Davis and colleagues (2014), who encourage adapting to the changing language used online. They advocate for informal, conversational, and semi-humorous tones that could

be used to start a conversation. The increased dialogue and cooperation can strengthen bonds between police departments and their communities.

Community Relations

The type of content posted on police-run social media accounts can vary, with the types of posts and content garnering various levels of engagement. While police departments have established that they will share informational posts about minor community events (Boateng & Chenane, 2020), there are attempts to experiment with various content to enhance engagement and relations with local communities. For example, the New South Wales Police Department's (NSWPD) use of social media engagement was dubbed a 'meme strategy' (Wood, 2020). The NSWPD experimented with posting memes and images of police animals to increase web traffic through their online profiles and to increase community engagement. This experiment on Facebook was used to capitalize on the environment, language, and culture of the internet to increase the attention these posts received. The goal of the strategy was to "introduce humor, to demystify and humanize the police force and to most importantly, link those posts to a serious message..." (Wood, 2020, p. 41). The police can be seen as an institution separate from the general public, and various means of social media attempt to bridge the gap between the two.

Police services will look at social media platforms and see methods for increasing community engagement and communication with the public (O'Connor & Zaidi, 2020). The purpose of communicating with a more open and transparent police department social media account was to increase citizens' participation in police matters (Bullock, 2018), akin to community policing. The idea of community engagement was for police

departments to build a rapport with the public while simultaneously allowing them to generate information that may be beneficial to criminal justice enforcement (Bullock, 2018). This framework follows that engagement begins with and ends with police departments and is used to advance policing goals.

Social media use among police departments can also be seen as an extension of community policing and is more likely to be implemented by agencies with this goal in mind (Hu & Lovrich, 2019). Community policing is typically referred to as the collaboration between the police and the general public. This type of policing encourages the conjoined efforts of these two groups in developing solutions to community problems (Shinta, 2019). Community policing focuses on enhancing the current social capital that police have with the public and wanting to build stronger communities where criminal events can be prevented or investigated with ease while also strengthening the public's trust in police institutions. Through police social media use, there are increased attempts at fostering a partnership between police agencies and the public (Hu & Lovrich, 2019).

Social Media Intelligence

Police departments and law enforcement agencies have the capability to collect data from online sources. It is estimated that 80% of local, state, and federal agencies use social media platforms as a medium to gather data and information from the public (Mateescu et al., 2015). The increasing activity on social media platforms has allowed for the congregation of data and information from vast sources. This information can take the shape of plain text posts, photos, or videos that individuals will share online for others to view and engage with. This engagement can take the shape of 'liking,' commenting on, or sharing the original content that is shared. Through this expanding spread of online

information, there exists the potential for police agencies to use this information about crime events.

The concept of social media intelligence (SOCMINT) for use in criminal justice was first coined in 2012 and is used to describe the analysis of information gathered from online social media platforms (Omand et al., 2012). SOCMINT can include text posts where a person of interest may express their intentions to commit a crime or post photographs of money or drugs obtained through illegitimate means. In addition to digital content posted online of individuals potentially engaging in criminal activity, SOCMINT can include abstract concepts, such as behaviors and sentiments. Since social media fosters the networking of similar interests, SOCMINT can focus on suspicious behaviors such as groups talking about dissent, collective calls to action (Dover, 2020), and other offline gatherings such as protests if there is reason to believe threats can occur (Melekain & Wexler, 2013). Intelligence gathered from social media platforms can expand beyond the initial data point to examining social network contacts. The gathering and analysis of online social media content forms the basis for Social Media Intelligence, used for criminal justice investigations and activities.

The social media information that can accumulate in online spaces is equated to 'crowd-sourced information' (Omand et al., 2012), which can be shared and easily spread between communities and the police. Individuals may do so because social media platforms facilitate conversations and online interactions between people and groups (Zeng et al., 2010), regardless of the topic. Information such as this is viewable to the public and anyone permitted by the poster. Since social media platforms encourage the spread of content and the desire for content to go 'viral' (widespread), individuals posting

information online may not consider privacy concerns and limit the audiences that can view what they are sharing. Since social media is considered crowd-sourced information, it is another form of data that observers can collect. The police can utilize this information to 'listen in on' individuals in online spaces (Bartlett et al., 2013). They typically may look out for informational cues or groups that could indicate online or offline criminal activity. Through listening to online data, the police could identify networks and groups, spot potential criminal events, or gauge public perceptions of specific actions/events (Bartlett et al., 2013).

Additionally, online content depicting criminal acts, interactions between groups, and activity patterns are not the only forms of SOCMINT. Certain specifics in the content itself can be used as criminal intelligence. For example, when any type of information is posted online, it is typically timestamped and could potentially contain a geotag (Andrew et al., 2018). This provides a specific date and time on when the information is posted and potentially where it was posted from. These specifics could assist law enforcement as a form of location identification for criminal events (Scassa, 2017) or for identifying potential crime pattern locations (Trottier, 2015). The desired crime events and patterns are not limited to a specific form of criminality; geotagging and location-based intelligence can expand through different fields of the criminal justice field. However, this information is notably used to assist in combating illegal online trade (Lavorgna et al., 2020). Human trafficking online is a focus of some research (Kapoor et al., 2017), but it expands into other areas and is used to combat the illegal trade of invasive species of flora (Lavorgna et al., 2020).

Research shows that there are efforts to automate this process and use algorithms and frameworks to search for the desired results. Proposed frameworks for identifying suspicious online activity include extracting data automatically from online sources (such as social media sites), screening information for potentially threatening speech/behaviors, and storing/codifying this information for further reference (San Biagio, 2021). Additional frameworks propose scouring various online information sources, not just content posts and speech online. Information can be detected through examining online advertisements hosted on social media or other platforms. Illicit activity and information can be (Kapoor et al., 2017) coded and disguised using obscure language to add some ambiguity. Proposed algorithms can continue to scour this information online and follow other frameworks for gathering intelligence.

The digital footprint that individuals leave can lead to creating their information profile, an online catalog that describes an individual active online (Rønn & Søe, 2019). Current research promotes that police departments exercise transparency and communication with the public surrounding their use of social media, whether it is engaging with the public, collecting data (Bartlett et al., 2013), or monitoring the online activities of the public (Mateescu et al., 2015). This form of accountability is encouraged to preserve and strengthen police legitimacy, while also ensuring to not undermine police legitimacy. When researching the use of social media intelligence, researchers note that proper guidelines be set in place that announce and limit the monitoring of online behavior (Bartlett et al., 2013), in addition to the type of information that is allowed to be viewed and can be used against individuals during the process of criminal investigation and prosecution (Mateescu et al., 2015).

Crime Analysts

Sworn police officers and non-sworn staff can use official police social media accounts regardless of training. Currently, training options are available (Melekain & Wexler, 2013) through policing services. Yet, law enforcement agencies may rely on self-taught practices and experience when tasking staff using social media (Brunty & Helenek, 2014). Crime analysts are supplemental staff within police departments that assist sworn police officers with their activities. Crime analysts' typical responsibilities involve assisting police by offering proactive policing strategies and allocation of resources by using data and intelligence (Brown & Ballucci, 2022). Typically, crime analysts focus on gathering geographic data to create tangible and accurate depictions of where crime hotspots may be present (Brown & Balluccci, 2022). This intelligence could then be used to assist police officers with their responsibilities.

The current understanding of crime analysis reflects a strong emphasis on criminal investigation as a common task within their job (Piza & Feng, 2017). In their work, Piza and Feng (2017) reflect that crime analysts commonly cite investigation as the main task they perform despite their established support methods. Crime analysis involves gathering data that can be analyzed and developed into a more digestible form of intelligence, such as detecting crime patterns to develop a crime hotspot map of a city (Belur & Johnson, 2016). This process involves gathering data from available sources, such as Geographic Information Systems (GIS), arrest/booking information, or potentially social media. Crime analysts are believed to be given the task of assisting police with investigation matters using whatever resources may be available (Piza & Feng, 2014).

Despite their established role, the current study will attempt to explore whether crime analysts have the potential to function outside of their traditional roles. This is based on their established experience with data collection, data analysis, and established dialogue with police officers. Crime analysts may be able to provide insight into how their job functions are adapting, evolving, and to what extent they are utilizing social media platforms and the internet.

Social Media Investigation

Social media platforms are spaces where online and offline crimes can be committed or detected (Bartlett et al., 2013). However, research surrounding the gathering of Social Media Intelligence (SOCMINT) and digital evidence has also emerged. With this form of data being collected from online social media platforms, it is currently being examined and analyzed for potential use in police activities, criminal investigation, and criminal prosecution (Brunty & Helenek, 2014). Police agencies possess the capability to use information gathered from social media to assist with surveillance, corroborating evidence, and investigative purposes (Brunty & Helenek, 2014). For example, when social media is used to assist with surveillance, there are currently limited standardizations for identifying suspicious individuals. Police can monitor individual profiles and use these as a network to branch out and potentially detect other individuals affiliated with similar suspicious activities (Brunty & Helensky, 2014).

Individuals who access social media and post information on these platforms are connected to the internet and have their own unique 'IP address,' which is a unique identifier that connects a device to the internet (Kalemi et al., 2017). Law enforcement

could use this data to link accounts and posts to a certain geographical location when given access to an IP address. Digital tracing and the use of social media geographical information also have the potential to be used by police departments. In a four-year investigation led by the New York Police Department (NYPD) in 2014, the use of social media data was reported to have led to the arrest of 103 alleged gang members (Patton et al., 2017). By concentrating their efforts on the neighborhood of Harlem, NY, the NYPD used online social media activities to create and categorize individuals into established gangs and cliques known to the area. Using online conduct found within social media spaces, the NYPD used this as a form of surveillance that could monitor and assist in investigating suspects they believed engaged in criminal activity (Patton et al., 2017). Since social media data is more consistently available and generated by the public, a steady stream of information can continue to be categorized by police. In addition to online surveillance, police and law enforcement are willing to subpoena social media platforms. When given access, police departments can view a wider variety of sensitive information, such as individuals' post history, uploaded photos, friends/followers list, and login information (Kalemi et al., 2017).

Data Mining

In addition to traditional methods of investigation, the use of data mining expands on this concept. Data mining involves a series of data collection steps that result in conceptualized usable forms of intelligence. This process involves collecting data (through a developed program/algorithm), classification of that data, identifying patterns and predicting outcomes based on those patterns, and representing that data that is usable and digestible (Sathyadevan et al., 2014). Data mining is built upon the foundation that

individuals have a modus operandi, a predictable method of action, and habits that can be categorized or used to develop a profile (Sathyadevan et al., 2014). While this method of collecting and analyzing data can be used to detect predictable behaviors and habits, it was initially developed to detect crime patterns within geographic locations (Nath, 2006). Developing crime patterns using data mining involves using specific algorithms designed to search for data, categorize it, and identify similar variables (Nath, 2006), like when developing criminal profiles. Based on these data mining methods, the information used in this process could be potentially derived from social media platforms, similar to what was found in the 2014 NYPD investigation and detection of Harlem gang members (Patton et al., 2017). The potential exists to gather, categorize, and visualize data from online social media platforms and use it to develop these same crime patterns or individual profiles.

In addition to digital tracing and data mining, social media data and SOCMINT can be gathered through a method known as 'web scraping.' This process involves using automated search tools that pour through and extract information from online sources, including social media (Farley & Pierotte, 2017). This method of online data collection could be used to collect information surrounding individuals or groups of interest, in addition to looking out for specific types of criminal events. Notably, web scraping is being used to assist in the countering of online human trafficking by identifying recurring posts, identities, and patterns found online (Farley & Pierotte, 2017). Web scraping, as a form of data collection, primarily focuses on the identification and creation of online identities that can then be transitioned into offline police activities (Andrews et al., 2018).

Individuals may not be aware that they are being monitored by police agencies based on the information they are sharing online (Scassa, 2017). Currently, there may be a level of expected privacy when sharing information on social media sites. Individuals may not be aware that their activity can be monitored by law enforcement. In the event the public is more widely informed by police monitoring their online social media activities, their information may still be compromised even after taking proper internet safety precautions. Police and other law enforcement agencies have established that they can legally obtain social media data from these platforms (Kalemi et al., 2017). Whether individuals are surveilled by the police through random scans or targeted, there still exists the potential for information posted online to be monitored by police or other law enforcement if they believe it can contribute to their activities and interests (Rønn & Søe, 2019).

CURRENT STUDY

Current research examines official police social media accounts as a means of communicating with the public to broadcast information and enhance community relationships. Police departments also use social media for data and intelligence purposes (SOCMINT). The use of social media data and SOCMINT to assist police and law enforcement in investigations is a popular technique among a sizable number of agencies (Fox & Rose, 2014). Currently unknown is how that data is gathered, used, and regulated by police departments. The current study has sampled crime analysts through the IACA and collected qualitative data regarding the gathering, implementation, and regulation of information gathered from online social media platforms. The primary qualitative data attempted to gain further insight into the type of data pursued, how it was gathered by crime analysts, from where, and what regulations or procedures were in place when examining the data collected.

Research Questions

The current research questions for this research project are as follows: (1) To what extent are crime analysts in the United States using social media platforms for data collection purposes? (2) When crime analysts use social media for data collection, how are they trained? (3) Of those crime analysts who did receive training, what are the best practices for data collection?

METHODOLOGY

In the current study, the author gathered qualitative data on how police departments conduct their gathering of social media data, if applicable. The current research surrounding SOCMINT and the use of social media platforms by police departments does not further examine how this data collection looks in its daily implementation. At this time the research reflects that police social media profiles will focus on communicating and broadcasting information to the public. Police social media accounts will post and share updates regarding traffic, public information, and events, alerts about missing people, and request information related to current crime events (Brainard & Edlins, 2015). However, further research also examines the possibility of social media being used as a means of collecting online information that can assist with real-world events. Social Media Intelligence (SOCMINT) is a term used to describe online crowdsourced information from social media sites (Bartlett et al., 2013). While the current research explored this potential for social media data, there is little practical information on how this data can be sought after, gathered, analyzed, and used to create real-world results for police departments.

Due to these circumstances, the current methodology made attempts to bridge this gap and explore how social media data is gathered and used in the current day-to-day tasks of crime analysts in the United States. Crime analysts are the focus of qualitative data collection due to the nature of their responsibilities and the collaboration that they have with their respective departments (Brown & Ballucci, 2022). Crime analysts will

perform data collection and create substantial graphs, charts, and maps that can easily be interpreted. This form of data collection is typically used to assist with the discovery of crime patterns and hotspots in the geographic area of their focus (Brown & Ballucci, 2022). The duties of crime analysts include creating tangible representations of raw data. The focus of this research has been the examination of how (or if) crime analysts will use social media to assist with their data collection, what information they seek, how they use the information that is found, and what the limitations are of using SOCMINT as a form of data.

Previous examinations of the collection of social media data revolve around the detection of language and vernaculars expressed online (De Smedt, De Pauw, & Van Ostayen, 2018). For example, hate speech that is directed towards a particular nationality or religious group can be studied to see how it could translate to real-world harm (Cohen et al., 2014). When attempting to investigate hate speech across social media platforms online, current research explores textual and linguistic analysis as a form of analyzing collected social media data. The data is found through developing policing methods that focus on detecting and capitalizing on 'weak signals online.' These weak signals are traces of information that can be a starting point that leads to more desirable results (De Smedt, De Pauw, & Van Osaeyen, 2018). In the case of social media data, weak signals would be content posted online that could lead investigators toward persons of interest's profiles online.

Police agencies could also choose to examine individual online profiles if there is reason to believe that these profiles could be linked to certain activities (De Smedt, De Pauw, & Van Osaeyen, 2018). Online profile pictures, profile names, names of places,

and rhetoric used online are all means by which weak signals can lead to more desirable results. Since the online digital landscape is home to an abundant amount of information, there is a need to streamline finding more desirable information and separating it from overwhelmingly irrelevant information. Social media data can function as an identifier for profiles and persons of Interest that could lead to offline criminal action. Examining social media data in this manner is studying how individuals will present themselves and behave online (De Smedt, De Pauw, & Van Osaeyen, 2018).

Textual and linguistic analysis are methods in which online speech, such as hateful posts on social media sites, can be detected. Text analysis involves breaking down the detected speech through a few methods that include translating their meaning, categorizing the sentiment detected into categories, mapping where the information posted originated from, and detecting common authors of these posts (Cohen et al., 2014). The purpose of text analysis is to identify behaviors online and is done by examining what people are saying online on social media. Linguistic analysis differs due to it focusing on behaviors exhibited by individuals of interest rather than the content itself that is posted. Linguistic analysis examines certain markers, such as the leakage of information online, the fixation that these individuals have with certain groups, and how these individuals identify themselves online (Cohen et al., 2014). Social media data can be used as a form of identification of potential behaviors, activities, and individuals.

Further, since social media is a form of crowd-sourced information online, it has the potential to create supplemental information for existing crime data. For example, since social media information can contain geographic information embedded in the content, this location data can be used to create population maps (Sanders & Condon,

2017). These maps can offer a stronger understanding of population centralization in relation to where crime is currently occurring (Malleson & Andresen, 2015). Using spatial crime analysis can assist with potentially creating population representations using the GPS data provided by social media posts. These population densities can be overlayed with existing crime maps where criminal events are occurring with improved location identification (Kapoor et al., 2017). This use of social media data offers the potential to examine where individuals are and what they are doing in relation to criminal events (Malleson & Andresen, 2015).

Based on the described foundation, the data collection process aimed to add further insight into the research through a series of binary, ordinal, and open-ended survey questions. The survey questions gathered qualitative data regarding how police departments conduct their data collection from online social media sites. These questions provided insight into the current day-to-day practices of crime analysts when navigating social media in official capacities (Brown & Ballucci, 2022). Notably, this study has attempted to expand how crime analysts use intelligence-based policing and utilize different fields of knowledge, such as social media data.

Survey

Before the start of the data collection process, approval from the Institutional Review Board (IRB) was needed for the survey to be sent out to possible participants. The purpose of IRB approval was to ensure the survey was reviewed by an administrative body and protect the welfare of possible human research subjects. A project was opened through the IRB's official website, where an outline of the project and a draft of survey questions were submitted for review. Based on the sample population, the extent of

information being asked of participants, and the potential for risk for participants, the IRB reserves the right to have projects reviewed by their committee. The current study was determined to be exempt from administrative review. Before the start of the survey, participants were provided with an informed consent form. This form would serve the purpose of outlining the scope of the study and how their responses will be used, as well as informing them of possible risks associated with engaging with the current study. The online survey was active for a period of two months. The online survey began in mid-March 2023 and lasted up until mid-May 2023, for a period of two months.

The survey questions are broken into five primary categories, which follow the roles of the police staff tasked with collecting social media data and how their agency directs data collection: *crime analysts, social media, data collection, data analysis,* and *limitations*. Refer to the Appendix for the full survey. The *crime analysts* section explores the task of performing data collection within police departments. Currently, crime analysis is a role that can be filled by sworn and non-sworn officers (Sanders & Condon, 2017). Additionally, regardless of whether these crime analysts are sworn or not, they are still capable of being certified through the IACA (Piza & Feng, 2017), which may reflect their work and capabilities as crime analysts.

While the role of a crime analyst is seen as a significant role in contributing to and strengthening a police department's database (Sanders & Condon, 2017), the role itself varies in perspective. In their work, Sanders and Condon also note that sworn police officers acting as crime analysts may perceive their role within the department as 'less than' and that their work is less beneficial. Regardless of the perceived value of their work, crime analysts are considered to serve an investigative purpose (Piza & Feng,

2014). The questions within this section will also explore the demographics and populations that these departments serve (Piza & Feng, 2017), which may affect the data that is available for them to collect. The demographics section differs from the rest of the survey as it provides predetermined answers for participants to choose from. The purpose of the demographics section will be to gain information that can be used to reflect the sample's participants.

The next set of questions, *social media*, explored how crime analysts interact with social media within their job functions. If applicable, these questions will inquire about the state of social media use in the department, the agency running these accounts, and communication with the public. Whether or not they are tasked with handling these official accounts, it will also explore how they are tasked with handling social media as part of their functions. As noted previously, crime analysts can be sworn or non-sworn officers, certified or uncertified, vary in education, and varied in training. There will be an examination of how the crime analysts' respective departments dictate the use of social media and how they prepare them for the tasks. The Toronto Police Service, for example, conducts structured training covering issues related to social media use (Melekain & Wexler, 2013). Additional research indicates that training in using social media sites is limited, and staff are mostly self-taught. This section will gauge the assistance given to crime analysts, if any, for them to complete their tasks.

The next set of questions explored the crime analyst's use of social media for *data collection*. While crime analysts' traditional roles are to collect data and transform it into tangible reports and charts, there is the potential for their work to take a more proactive approach (Sanders & Condon, 2017) by using social media data. When permitted, how is

this form of data collection performed, and are analysts given the proper tools to manage sophisticated analysis or research that varies from traditional tasks?

Data analysis followed social media data after it was collected by crime analysts. The interviewees were asked to describe the type of information that is gathered, what that process looks like, and what the results encompass. Social media data can contain helpful information (such as geographic locations) and be used as a source of intelligence. What are the current day-to-day results of this form of data collection? Per the work of Piza and Feng (2014), crime analysts serve to assist with ongoing investigations. How are they serving this purpose and utilizing social media data? Additionally, how is this information determined to be helpful in the overall goals of the police department? Are crime analysts contributing digital evidence or intelligence that is passed along to law enforcement agents? Or does social media act as a tool for surveillance that allows for the tracking of individuals that are deemed of interest to the police department for additional operations (Brunty & Helenek, 2014)? Overall, current research reflects that there is potential for social media to contribute to the field of social media intelligence. What does that look like on a practical scale?

Limitations examined the concerns that follow the involvement of police on social media platforms. Police activities in any capacity must hold some ethical ground and transparency to maintain public trust and police legitimacy (Bartlett et al., 2013). When navigating social media and collecting data for police purposes, what legal considerations do crime analysts keep in mind? Additionally, what policies and procedures are set in place by the police department themselves, and how could they be delegating tasks to be conducted in online spaces (Melekain & Wexler, 2013)? Further, the following questions

will explore what barriers, if any, crime analysts may face when attempting to collect data from online sources and social media platforms. This includes barriers such as privacy settings, departmental policies, and ethical concerns.

Analytic Strategy

The foundation of the current study was based on qualitative research methods and data analysis methods. The current study has taken an inductive approach and the author collected primary data, which is the online open-ended surveys completed by crime analysts within the United States. Rather than being based on theory, the current study attempted to create meaning from the newly collected data (Bingham, 2023). For instance, crime analysts who repeat similar techniques, experiences, or tools will help develop themes regarding their practices when using social media. The current study developed themes and created findings based on the data collection process results (Bingham, 2023). After the data collection process, the data has transformed to create possible explanations for the use of social media data by police departments and crime analysts. This process involved coding responses through two-cycle coding. This form of analysis differs from deductive approaches, which is the application of theory in testing data. Data was not sorted into predetermined categories or themes; rather, the themes were transformative from the data (Saldana, 2014, p. 22). In the current study, the crime analysts shared information and their experiences that were used to help explain the process by which social media data is collected, analyzed, and implemented within police departments.

The methods used in the study were two-cycle coding, which focused on the development of codes through critical analysis and synthetizations (Tracy, 2013, p. 194).

The two-cycle coding method involved the examination of prominent and latent meanings within the data through primary and secondary coding stages, which led to the development of emergent themes (Tracy, 2013, p. 188-194). This process involved developing primary codes, or *a-priori* codes, within the first cycle. These codes developed from the research questions posed in the current study. *A-priori* codes focused on 'what' was present within the collected data and operated under the expectation that crime analysts were going to discuss certain topics related to social media data collection practices.

Through the second cycle, secondary codes were developed after reviewing the collected data set. The responses from crime analysts were examined and evaluated for what they were reporting within the survey. During this stage, coding methods were implemented to further develop the emerging codes (Tracy, 2013, p. 188-194). After the second cycle and the evaluation of the emerging codes, emergent themes began to develop from the data set. Emergent themes characterize the codes found and create themes that are reflective of the data set (Tracy, 2013, p. 188-194).

The development of themes involved the use of inductive coding methods. These methods of coding used the data set as a starting point, from which codes emerged as the flow of information continued to pour in (Bingham, 2023). These coding methods were used due to the emerging research regarding the use of social media data by crime analysts. The coding process translates initial large data sets into smaller, digestible, and understandable categories. The coding process took the survey responses from all 87 respondents and categorized them using descriptive coding and structural coding methods. Additionally, in vivo coding was also utilized on a smaller scale. This coding

method involves using the ‘actual language’ found in the collected data (Tracy, 2013, p. 190). In vivo coding was used to preserve the language used by crime analysts and used their exact responses as a reflection of the current study.

Descriptive coding involved condensing the collected online surveys into simple phrases that captured the ideas answered within the questions asked (Saldana, 2021, p. 88). Crime analysts who responded using simple phrases, similar ideas, or identified similar practices were sorted using similar codes. For example, when crime analysts were asked about how social media data was used, the open-ended responses were sorted into different categories that captured the ‘essence’ of what was being reported. Crime analysts may report similar accounts when describing the use of social media data, which can then be broken down into more specific methods. Descriptive coding is preferred when attempting to ‘make sense’ of the data being analyzed (Saldana, 2021, p. 88)

While descriptive coding breaks qualitative data into categories, structural coding was used to preserve the structure of the collected data. Structural coding involves the labeling of sections of data that may be referred to at a later time and assists with keeping track of larger data sets (Saldana, 2021, p. 84). In the current study, structural coding was used to segment data and keep themes accessible while comparing topics. For example, the responses for different pairs of questions were paired together to create emerging themes, and structural coding was used to keep track of categories of thought when compared against responses to differing questions. When examining the training available that would prepare crime analysts to use social media, the responses to this question were compared to the responses from a question that inquired about the tools that crime analysts may use when collecting data from social media. Structural coding is

preferred when the analysis process is driven by certain topics or ideas that are converging across differing codes (Saldana, 2021, p. 87).

Although it plays a smaller role compared to the previously discussed coding methods, In vivo coding was also utilized in the current study. In vivo coding involves using the actual language found within the data set, using respondents' language verbatim (Saldana, 2021, p. 91). This is crucial for pulling direct quotes from crime analysts. The purpose of the study was to gain further insight into the evolving practices of using social media data. Therefore, it was crucial to pull certain responses as is. Direct quotes help encapsulate the themes found within the current study and carry a level of impact as they capture the essence of the study.

Sample

For data collection, the developed survey questions were administered to crime analysts through the Internal Association of Crime Analysts (IACA) and remained active for a period for two months. The IACA is a professional non-profit organization that is composed of crime analysts from across the globe. The goal of this organization is to offer training and experience to those in the crime and intelligence analyst fields to strengthen those professions. Since the IACA is composed of crime analysts, intelligence analysts, and police officers from across the world, the members of this organization can provide significant insight into the research questions. Permission was sought from the IACA to reach out to its members and inquire if they would allow for the survey to be sent out. Permission to post the survey onto the IACA forums was permitted under the condition that the requester had an active membership with the IACA. In total, 116 crime

analysts responded to the call and 87 participated in the survey to completion. Thus the analytical sample consisted of 87 participants.

In addition to posting on community boards, further inquiries were made with fifteen regional associations and agencies[1] within the United States that the IACA has networks. These smaller regional associations exist to create compact networks where crime analysts within their regions can share information, establish standards and goals, or report on trends in criminal activity. When reaching out to these agencies, the scope of the project was explained to responding webmasters or secretaries for these chapters. When permission was granted, the survey was distributed via email by the agencies' respective members, along with an informed consent document.

Further, the IACA maintains a membership directory on its website that is available to be viewed by members of the organization. The author utilized this membership directory to compile a distribution list of emails for crime analysts. When using the membership directory, email addresses for crime analysts were sought out and compiled for distribution, with no other personal identifiers being recorded or used. Prospective participants would receive an email (unless accessed through the IACA forums) that contained information detailing the survey project, an informed consent document, and an electronic link that would direct them to the survey that they could

[1] Florida Crime & Intelligence Analysts Association (FCIAA), Carolinas Crime Analysis Association (CCAA), Virginia Crime Analysis Network (VCAN), Mid-Atlantic Regional Association of Crime Analysts (MARACA), New York Association of Law Enforcement Analysts (NYALEA), Massachusetts Association of Crime Analysts (MACA), Mid-America Regional Crime Analysis Network (MARCAN), Crime Analysts of Illinois Association (CAIA), Wisconsin Law Enforcement Analyst Network (WILEAN), Midwest Association of Criminal Intelligence Analysts (MACIA), Texas Law Enforcement Analyst Network (TXLEAN), Colorado Crime Analyst Association (CCAA), Northwest Regional Crime Analyst Network (NORCAN), Arizona Association of Crime Analysts (AACA), California Crime & Intelligence Analysts Association (CCIAA)

complete at their leisure. The current survey composition includes 23 survey questions (refer to Appendix). The questions are designed to be optional and allow for multiple-choice and open-ended responses if the questions are relevant to their current work or experience with using social media to collect data used by their respective police departments. While there is a section for demographics, the developed survey is confidential. The only identifiable information is the interviewee's email address linked to their IACA membership, which will not be shared or used for further research.

Qualtrics

When developing the open-ended survey that would be used to gather data, Qualtrics was chosen as the survey tool. This software was chosen as it offers extensive customization options available for survey development, in addition to its ability to host and send the survey to the respondents through a link. Qualtrics has the potential to compile a distribution list of email addresses and send them in mass to potential participants. Additionally, Qualtrics hosts and stores the responses during the data analysis period once surveys are completed. The data collection survey, which was hosted through Qualtrics, will remain active for two months. During this time, invite links and emails will be distributed, and potential participants may complete the survey at their leisure.

RESULTS

The current study has attempted to explore practitioners in the field of criminal justice and their practices in online social media spaces. Through qualitative interviewing, the perspectives of crime analysts in the United States were gathered to understand how and if they navigate social media platforms for data collection purposes. The data collection process yielded a total result of 87 responses from crime analysts in the United States. The responses from crime analysts provide further insight into their roles as practitioners, the training that they may undergo, the process in which social media data was collected, possible tools and programs utilized, and the realities of using social media information as a source of data for law enforcement agencies. Further questions explored topics relating to the perceived benefits of collected data as well as the barriers that may inhibit data collection on social media platforms. The results of the data collection process are reflective of the research questions posed, including: (1) To what extent are crime analysts in the United States using social media platforms for data collection purposes? (2) When crime analysts use social media for data collection, how are they trained? (3) Of those crime analysts who did receive training, what are the best practices for data collection?

Research Question #1

Throughout the data collection process, the prevalence of social media within police departments in the United States became apparent. Police departments in the United States are utilizing social media for many purposes and to achieve various goals.

Results report that police departments have a significant presence on social media platforms, with the platforms of choice being predominantly Facebook (50 responses), Twitter (46 responses), and Instagram (34 responses). Not only were these major platforms used most often, but it is quite common and likely that police departments will not limit their activity to just one platform but may have an active presence on a variety of social media platforms. Crime analysts report that their police departments are not only active on social media platforms but post a variety of information and engagement through their pages. Social media was mainly used for public awareness (44 responses) and community outreach (34 responses). Police departments aim to take an active role online and attempt to share a variety of information with residents residing in their jurisdiction. Information such as traffic alerts, public safety information, sharing information regarding ongoing cases and investigations, and providing crime education to the public. In addition to public awareness, police social media activity is a form of community outreach that attempts to create a dialogue between the police and the community that it serves.

Despite the rising presence of police departments on social media platforms, the practice of using such platforms to collect data is still limited and has received polarizing results. Of the fifty-seven responses, thirty respondents (52.63%) reported that they did not use social media for data collection purposes, while twenty-seven respondents (47.37%) reported that they did use social media for data collection purposes. As seen in Table 1, these results indicate that there is not an established precedent for utilizing social media for data collection purposes. Twenty-seven crime analysts reported that they do implement these practices in their daily activities. Meanwhile, more than half of crime

analysts report that they do not implement these practices. Whether this is attributable to crime analysts being unaware of these practices or data collection tools existing is unclear. A lack of implementation of social media data collection practices may also be attributed to departmental restrictions that prohibit these practices, a lack of standardized training, or even a lack of tangible return on investment for the implementation of these practices.

Table 1. Crime analysts' demographics.

Variable	**n**	**%**
Gender		
Male	6	26.09
Female	17	73.91
Non-binary	0	0.00
Prefer not to answer	0	0.00
Total	*23*	*100%*
Age		
18-25	1	4.76
26-35	7	33.33
36-45	9	42.86
46-64	3	14.29
65+	1	4.76
Total	*21*	*100%*
Level of Education		
Some High School	0	0.00
High School Diploma	0	0.00
Bachelor's Degree	7	30.43
Master's Degree	15	65.22
Ph. D. or higher	1	4.35
Total	*23*	*100%*
Years spent as a crime analyst		
> 1 Year	5	8.77
1-3 Years	23	40.35
4-9 Years	22	38.60
10+ Years	7	12.28
Total	*57*	*100%*
Does your agency use social media for data collection purposes?		
Yes	27	47.37
No	30	52.63
Total	*57*	*100%*

Research Question #2

Despite less than half of crime analysts reporting that they do implement a form of social media data collection, the question remains as to how they are trained for this responsibility. When inquiring about the training available to crime analysts to prepare them for using social media, many crime analysts (26 respondents) indicated that they do not receive any training. Followed by crime analysts (21 respondents) who reported that they did receive training. However, it was provided through third-party agencies rather than internally within their police departments. Internal training for social media use was available for some crime analysts; however, it was minimal (nine respondents) and was not standard practice for training crime analysts on how to navigate and use social media platforms for data collection purposes. Internal training took a variety of shapes: shadowing and learning from experienced crime analysts, reviewing training materials found in departmental handbooks, and utilizing existing knowledge that carried over from times at previous police departments.

Most of the training available was offered through a variety of third-party sources. Crime analysts reported having access to online resources, such as memberships to the International Association of Crime Analysts (IACA), where they have access to training modules and training webinars, as well as access to forums where questions and inquiries could be posed to other fellow crime analysts. Crime analysts reported signing up and utilizing any available training that they believed could be applicable and assist with their positions and using social media platforms, pending approval from their departments. In addition to online resources, responses also indicate crime analysts utilizing conferences and training offered through differing agencies, such as training available through the

Federal Bureau of Investigation, Drug Enforcement Agency, or even open-source intelligence training offered through the National Initiative for Cybersecurity Careers and Studies (NICCS). Access to these forms of training and seminars is inconsistent, with some crime analysts reporting that their attendance for such training is dependent on their access and knowledge of these training taking place and can also be dependent on funding approval from higher-ups within the department.

Among the third-party training reported by crime analysts, Open-Source Intelligence Training (OSINT) was mentioned specifically (seven responses). Offered through the NICCS and the McAfee Institute, Open-Source Intelligence Training intends to train police practitioners in collecting and analyzing publicly available data online, such as information posted on social media websites. This training offers the opportunity for students to learn about the basics regarding open-source intelligence, how to collect information, how it can be used, as well as moral and or ethical aspects when working with publicly available information. Through OSINT training, practitioners can be trained on how different open-source tools are used and how to conduct investigations using open-source intelligence. OSINT remains accessible to police practitioners and students interested in learning more about the subject. However, access to training is available to parties who pay for the course and certification.

Overall, the standardization of training for social media data collection is in its infancy. Collected data results indicate inconsistencies in the training process for crime analysts to become familiar with data collection through social media platforms. Training is not always available for crime analysts. When available, it is typically through third

parties and other agencies, often at the discretion of crime analysts themselves, to seek out and sign themselves up. One crime analyst reported:

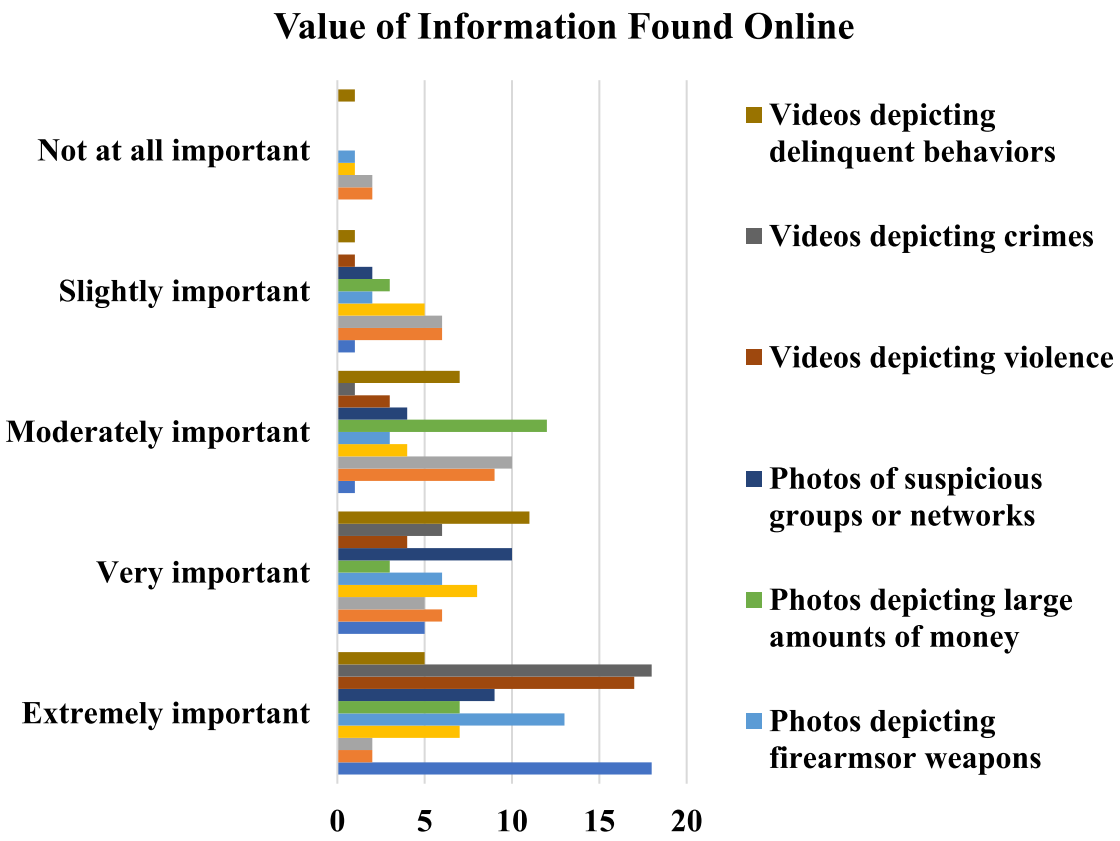
> We don't run the PD's social media, but we do have other social media accounts that we monitor for potential threat to the PD and citizens of Rock Hill. No training is provided, just use and experience on my own social media accounts. Some databases I have access to provide free trainings for social media analysis that I've done in the past. (Respondent 73)

Research Question #3

Training, certifications, and seminars are not a guarantee for crime analysts. However, when they are available, tools and programs are available that can act as best practices for crime analysts when collecting data through social media platforms. Text posts, digital media, and other activities posted on social media platforms are considered public information and may contain an overwhelming volume of information for crime analysts to sort through. Individuals can post a variety of information at a consistent rate, which could hinder or overwhelm crime analysts when searching for data they may consider intelligence. What information is considered valuable information, and what information is considered unimportant to crime analysts? Respondents noted that the information that was considered *extremely important* were social media text posts that contained threats of intended violence, videos posted online depicting violence, and videos depicting criminal events. Videos posted online depicting delinquent behavior posted photos of weapons, firearms, and drugs were considered V*ery Important*. Little information was considered *not important at all*. While all information related to criminal justice posted online could be considered slightly important, there is information that is considered more important and could assist law enforcement more. Crime analysts prioritize the gathering of information that explicitly depicts crime occurring or is related

to criminal activity. The most important online activity that crime analysts searched for were text posts that depict threats of intended violence and videos depicting crimes occurring.

Figure 1. What type of information do you consider important when collecting data?



After identifying the types of information and data crime analysts consider valuable for law enforcement officers, what are the best practices for collecting this online information? Crime analysts report utilizing a variety of tools and programs to assist with the data collection process. Notably, crime analysts reported using simple Microsoft Office programs and media screen capture tools (such as snipping tools). Using these basic programs, crime analysts were able to screen capture and collect images of online posts they considered important enough to archive. Additionally, crime analysts

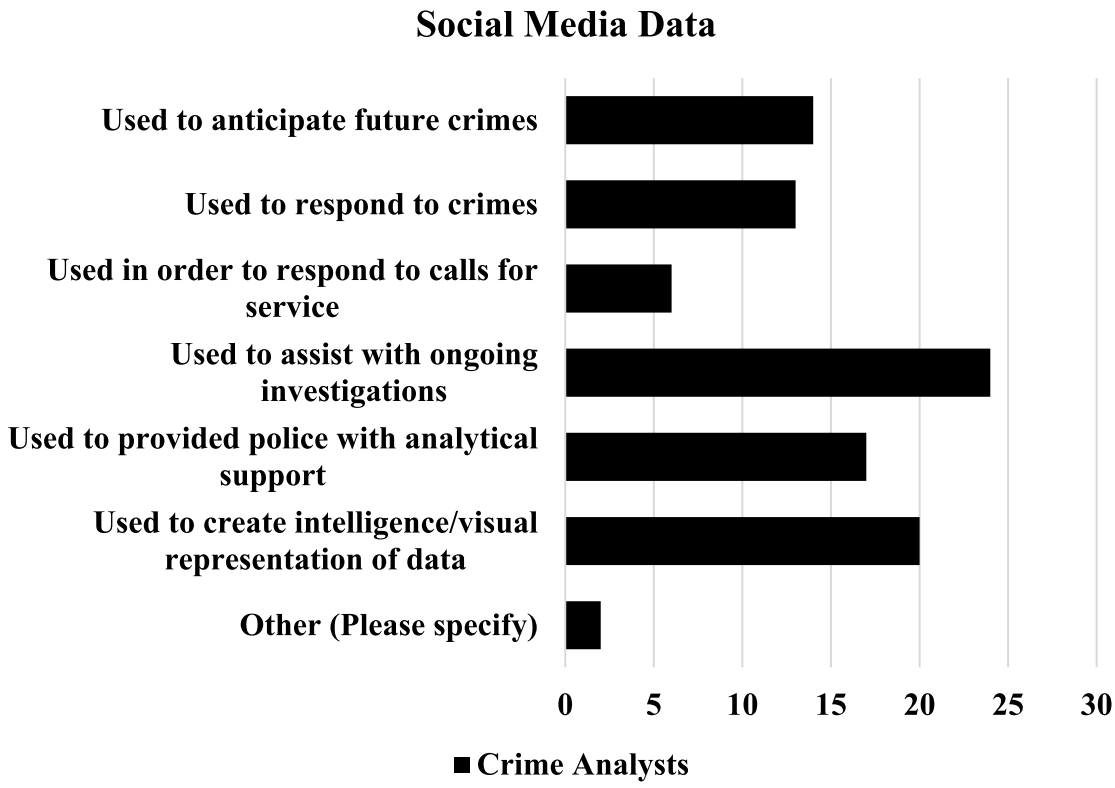
report simply using ‘copy’ and ‘paste’ to export information they found on social media and transfer it into a Microsoft Word document. These basic tools and data collection techniques offer crime analysts a straightforward means of saving information they may find online with minimal effort or training needed. This process, however, is manual and requires crime analysts to collect information themselves.

Although basic collection tools and methods are available, crime analysts also noted data collection software available that could assist with the handling of substantial amounts of data for them to analyze. Programs such as Geotime Enterprise and PenLink (PLX) assist individuals in searching for, collecting, and analyzing information that they are interested in using as possible intelligence for police. Data collection software and analytical tools such as these are designed for law enforcement use and provide the tools that they may need to automatically collect open-source information and assist with investigations. Manual data collection is time-consuming and requires active input from crime analysts to gather the information that they need. Meanwhile, data collection software and analytical tools such as PLX and Geotime Enterprise were designed to be time-effective and provide automated data collection. These tools can assist practitioners in expanding their tasks in the field of digital investigation and making sense of previously unusable data. For example, rather than manually collecting data and sifting through the information, programs like PLX assist practitioners with collecting and analyzing desired data in real-time, whether this is searching through historical data or information that is being posted live on social media sites. Additionally, once collected, these data collection software assists in the creation of visual representations of data and the creation of intelligence that can be used by their respective police departments. Please

refer to the appendix for a table outlining the reported data collection tools, the services they offer, and accessibility.

Once information is collected from social media using data collection software or other manual data collection processes, it may be used by police departments in a variety of manners. The current data reflects a few ways in which crime analysts will want to utilize social media data. The most prominent use of social media data is to assist police departments with ongoing investigations and the creation of intelligence for police to use while on patrol, as previously discussed. However, social media data holds possible potential for law enforcement agencies to be proactive and reactive with the intelligence they receive online. Using gathered data online, it could be used to respond to crimes that have occurred, as well as anticipating future crimes. For example, if individuals post credible threats online that are reported to the police, they can choose to act on that tip and proactively investigate possible suspects. In addition to online crime tips, one crime analyst noted that the information they gathered online was used in "advising precincts about upcoming gang events, funerals, large car meets & gatherings" (Respondent 42). Information posted online on social media sites can act as a new source of information for law enforcement, a tip line that they can use as the basis for a new investigation.

Figure 1. In what ways is social media data used once it is collected?



DISCUSSION

Policy Implications

Regarding the results of the data collection process, there are future implications for future research, policy, and practices in the field of using social media for data collection purposes. As previously explored, the current landscape of social media use exists to communicate with the public, with newfound online territories being explored. Crime analysts have discussed the potential for further social media use in ways that can provide benefits to the police departments they service. However, there are still some implications for future policies to address. For researchers aiming to further investigate this field, there is still a significant gap in knowledge regarding the practice of collecting data from social media. The current study explored the prevalence of collecting social media data and what that practice may look like. Further evaluation of the field is still needed. Crime analysts report that they utilize social media as part of their job tasks. However, the discretion that they have when using these platforms is still unknown. Crime analysts did not report the tasks handed down to them by higher-ups or the chain of command when attempting to collect information online from social media. Current data shows that collecting social media data is not a strong and standardized practice in the United States. However, there is potential for that to change. In addition, some tools could be implemented to assist with the implementation of this practice.

Regarding policymakers, the practice of collecting social media data could benefit from a standardization of practices. As previously discussed, there are inconsistencies with the training available to crime analysts when preparing them for social media use and data collection. Analysts reported few if any training opportunities or programs that could prepare them for using social media to collect data within their departments. Few had existing knowledge of how to do so, but this existing knowledge was either self-taught or carried over from previous agencies. However, a sizable portion of respondents also noted that any training that they received was via third-party sources, such as governmental agencies, neighboring policing departments, or courses online. Notably, when asked about available training, one crime analyst commented: "If we can find training, we can apply to go (funding limited). Otherwise, none" (Respondent 34). Future policies could implement standardization of training and tools for crime analysts who wish to expand their practices in the field of digital investigation and social media data collection. Open-Source Intelligence Training and some data collection software offer training that is attached to tools that can prepare crime analysts for gathering and analyzing online information.

Training and tools are available for practitioners interested in implementing social media data collection in their police departments. As previously discussed, programs and training are available and designed with law enforcement agencies in mind. Training programs and tools such as Geotime and PLX take into consideration the type of information and data that crime analysts have a vested interest in. Additionally, they offer tools and analytical support that make this form of practice more easily accessible and implementable in police departments. Future policy could be used to raise awareness of

this practice. Crime analysts may not be using social media data collection due to not knowing that this practice exists and is accessible due to tools and programs. Crime analysts may not be using social media data collection due to a lack of tools, training, or knowledge of the practice. However, these practices are accessible and available for police departments who are interested in expanding into this field of digital investigation.

Limitations

The current study attempted to sample individuals employed as crime analysts in the United States. Within the scope of the current study (116 starting participants, 87 completed surveys), the results are limited in the external validity of the target population. This study attempted to survey the target population and collect qualitative data regarding crime analysts' current use of social media data collection, contingent on their implementation of these practices. The data collection process resulted in additional insight into the practices of crime analysts and their familiarity with collecting online data from social media platforms. However, their results are not reflective of all crime analysts' practices within the United States. The methodology was designed to cast as wide of an online net as possible and made a variety of attempts to capture a diverse sample of crime analysts in the United States. This included sampling the IACA and other regional crime analyst agencies that operate within the United States, as well as contacting individual crime analysts who were associated with the IACA. Further studies on this subject should further explore these means of contacting crime analysts to capture a wider sample size and increase the external validity of results. Past studies that have also examined crime analysts have had varying sample sizes. A 2010 study of crime analysts yielded a total sample size of 18 crime analysts (Burrell & Bull, 2010).

Additionally, another study years later yielded a significantly higher sample size; 163 crime analysts were able to be interviewed (Piza & Feng, 2017). During these previous studies, there is a variation in the total crime analysts able to be sampled, with the current study falling between the previous explorations into the topic. Future studies, regardless of sample size, should attempt to procure a nationally representative sample of analysts reflecting different regional practices.

Future Directions

The responses and themes that have been presented in this study invite further discussion regarding the use of online data by law enforcement agencies. Whether this data and information come from social media platforms or other sources online, individuals create online data trails that are open-sourced and can be easily accessible to law enforcement agencies if privacy precautions are not taken. Throughout the data collection process, a prominent limitation discussed was the inability of crime analysts to collect data from social media platforms due to user-enabled privacy settings. Crime analysts noted that these settings prohibited further data collection on desired profiles, thus "making it impossible to acquire any useful data" (Respondent 79). On popular social media platforms (such as Facebook, Instagram, and Snapchat), users are provided with settings that allow the customization of which information is publicly viewable and which information is private. Once approved, 'friends' or 'followers' are permitted to view privatized posts and profiles. These settings allow users to control how their profiles are viewed while omitting their profiles and activities from being viewed by anyone not approved of by the profile's owner. If privacy settings were enabled, these could provide a hurdle when crime analysts explored online breadcrumb trails. Crime analysts did

report instances of utilizing the court system to bypass privacy settings, but few crime analysts reported that court subpoenas could be used to obtain the pertinent information needed from social media platforms. However, this process can be lengthy and is not discussed in depth. If the court is not involved, crime analysts are unable to view private profiles unless their accounts are approved, and the user accepts the 'follow' or 'friend' request.

While user privacy settings may deter crime analysts from viewing and collecting information from private profiles, they may not be the complete solution for individuals online. Crime analysts report that these privacy settings may function as a limitation, but policies regarding the creation of fictitious accounts or profiles for the sole purpose of bypassing privacy settings are inconsistent. Notably, one crime analyst reported:

> Dept policy does not allow us to use our fictional accounts to 'friend' anyone in an effort to see posts or info that has been restricted or private access. Otherwise, if it is readily available to the public, it's fair game for us to collect and use. (Respondent 63)

The decision by police departments to prohibit the creation of fictitious and 'undercover' social media profiles is at the discretion of individual police departments. Currently, crime analysts do not report legal policies that prohibit how they collect online social media data. Regulations that prohibited how social media data could be collected were implemented by individual police departments, which was still uncommon and underreported. The primary limitation that prohibited the collection of online social media data was privacy settings enabled by the user rather than legal or departmental policies aimed at protecting individual privacy.

Future research could explore the privacy concerns users may have when posting information online on social media platforms. As previously noted, departmental and legal policies are not standardized; information that is posted online may be publicly available and free for police departments to use as part of their investigation or practices. Social media users may not be aware of the access law enforcement agencies may have online and the scope of the information they are allowed to collect and use. As discussed previously, while crime analysts aim to use collected social media data to create intelligence and provide analytical support to police, they also aim to use this data to assist with ongoing investigations, anticipate future crimes, and respond to ongoing crimes. Future research could explore the caution that social media users may need to exercise before sharing or posting information online on social media sites.

Additional further research should explore the limitations that prevent crime analysts from applying social media data collection practices into their tasks. As noted in the current study, crime analysts did not overwhelmingly report that they engaged in social media data collection, nor did they predominantly report they did not engage in these practices. Social media data collection trainings, software, and tools exist that may assist crime analysts and other police practitioners with its implementation. However, the limitations and barriers that may prevent social media data collection are still unknown. Future research should explore crime analyst's police department's geographic locations and department sizes, and how this may affect the implementation of social media data collection. Police department sizes may vary among cities, counties, and states; the size and resources available to police departments may influence their ability to access social media data collection trainings and software. Despite a crime analyst being aware of

these data collection practices, the proper execution of these practices may be limited by departmental funding. Future research should explore which police departments can access social media data collection training in addition to which departments have access to data collection software, then compare that to where those departments are located within the United States.

Conclusion

The practice of collecting data from social media platforms is an emerging practice that still holds potential for future researchers and practitioners. Through the current study of crime analysts in the United States, it was found there are inconsistencies with the implementation of social media data collection, training available to prepare crime analysts for navigating social media and collecting information, and the use of tools and programs to effectively collect information. While some agencies do not currently engage in this practice, other police departments do. When available, crime analysts can attend and compete with third-party training and utilize a variety of tools and data collection software that assist with the analysis of online information. Crime analysts report value in the information that is posted online on social media, whether it is written threats online, digital media of drugs or other illegal substances, or even digital media of crimes that are occurring. When coming from a person of interest or a criminal suspect, all information has varying usefulness for crime analysts. This information can not only be used to reactively respond to crime and other ongoing calls for services but can function as the foundation for future investigations. Crime analysts report the potential for online social media data to provide leads for future investigation or act as criminal intelligence.

APPENDIX

Crime Analysts

- Are you a police officer or civilian analyst?
- What is the approximate population of your jurisdiction?
- How many years have you spent as a crime analyst?
- How much of that time has been with your current agency?
- What are your tasks and responsibilities as a crime analyst?

Social Media

- Does your agency have any official public social media accounts?
- What platforms is your agency active on?
- Currently, how does your agency utilize social media and for what purposes?
- What training(s) (if any) does your agency offer to prepare you or other crime analysts for using social media within your role?

Data Collection

- Does your agency use social media for data collection purposes? *
- What are the perceived benefits of using social media as a form of data collection? In what ways does this assist you in crime analysis?
- What type of information online do you consider important when collecting data?
- What does the process of collecting information/data from social media platforms look like?

Data Analysis

- What tools, programs, or software are available for you to use when collecting data from social media platforms?
- In what ways is social media data used once it is collected?

Limitations

- How much would you agree that the following barriers limit your ability to collect information and data from social media sites?
- If applicable, please describe in detail some of the issues mentioned above.

Demographics

- What is the year of your birth?
- What is your gender identity?
- What is your level of education?
- What is your ethnicity?

Data Collection Program	***Services offered***	***Possible cost***	***URL link***
PenLink (PLX)	Live data collection, Historical Autoloads, Advanced Analysis, Data Integration	Demos are available, cost is adjustable to fit agency size and budget	https://www.penlink.com/
Geotime Enterprise	Live data collection, automated reporting, mapping for data, data analysis,	Demos available	https://www.geotime.com/enterprise-1
Cellebrite	Collect digital intelligence, assist with investigations and analysis, create reports for prosecution	Program customizable to fit agency size	https://cellebrite.com/en/home/
Hunch.ly	Web capture tools, automated documentation, create reports for prosecution, mobile platform available	Demos are available, cost is adjustable to fit agency size	https://www.hunch.ly/
Cobwebs	Live data collection, automated web investigation, assist with investigations and analysis, generate real-time alerts	Demos are available	https://cobwebs.com/en/
Chorus	Assist with digital investigation and data analysis, automated data collection, create reports, data integration	Demos are available	https://chorusintel.com/
CLEAR	Identify persons of interest, assist with investigations, create reports for prosecution	Demos are available	https://legal.thomsonreuters.com/en/products/clear
TLOxp	Access to open-source information data bases, build reports of connected individuals, social media searching, address reports	Demos are available	https://www.tlo.com/

REFERENCES

Aguilar, G., Ompolasvili, S., Amaya, L. G., & Kerstens, S. (2021). True crime TikTok: Affording criminal investigation and media visibility in the Gabby Petito case. *Masters of Media*, *29*.

Andrews, S., Brewster, B., & Day, T. (2018). Organised crime and social media: a system for detecting, corroborating and normalizing weak signals of organised crime online. *Security Informatics*, *7*(1), 1-21.

Bartlett, J., Miller, C., Crump, J., & Middleton, L. (2013). Policing in an information age. https://indianstrategicknowledgeonline.com/web/DEMOS_Policing_in_an_Information_Age_v1.pdf

Bingham, A. J. (2023). From data management to actionable findings: A five-phase process of qualitative data analysis. *International Journal of Qualitative Methods*, *22*, 16094069231183620.

Boateng, F. D., & Chenane, J. (2020). Policing and social media: A mixed-method investigation of social media use by a small-town police department. *International Journal of Police Science & Management*, *22*(3), 263-273.

Brainard, L., & Edlins, M. (2015). Top 10 US municipal police departments and their social media usage. *The American Review of Public Administration*, *45*(6), 728-745.

Burrell, A., & Bull, R. (2011). A preliminary examination of crime analysts' views and experiences of comparative case analysis. *International Journal of Police Science & Management*, *13*(1), 2-15.

Brown, E., & Ballucci, D. (2022). Specialized knowledge: Understanding crime analyst's roles and responsibilities and the impact of their work. *Criminology & Criminal Justice*, 1-17. 17488958221095980.

Brunty, J., & Helenek, K. (2014). *Social media investigation for law enforcement*. Routledge.

Bullock, K. (2018). The police use of social media: Transformation or normalisation? *Social Policy and Society, 17*(2), 245-258. doi:10.1017/S1474746417000112

Cohen, K., Johansson, F., Kaati, L., & Mork, J. C. (2014). Detecting linguistic markers for radical violence in social media. *Terrorism and Political Violence*, *26*(1), 246-256.

Davis, E. F., Alves, A. A., & Sklansky, D. A. (2014). Social media and police leadership: Lessons from Boston. *Australasian Policing*, *6*(1), 10-16.

Dekker, R., van den Brink, P., & Meijer, A. (2020). Social media adoption in the police: Barriers and strategies. *Government Information Quarterly*, *37*(2), 1-9.

De Smedt, T., De Pauw, G., & Van Ostaeyen, P. (2018). Automatic detection of online jihadist hate speech. *arXiv preprint arXiv:1803.04596*.

Dover, R. (2020). SOCMINT: A shifting balance of opportunity. *Intelligence and National Security*, *35*(2), 216-232. https://doi.org/10.1080/02684527.2019.1694132

Farley, E., & Pierotte, L. (2017). Web scraping: An emerging data collection method for criminal justice researchers. *Justice Research and Statistics Association*.

Fox, R. L., & Rose, M. (2014). Public engagement with the criminal justice system in the age of social media. *Oñati socio-legal series*, *4*(4), 771-798.

Goldsmith, A. (2015). Disgracebook policing: Social media and the rise of police indiscretion. *Policing and Society*, 25(3), 249-267.

Hsieh, H. F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research*, *15*(9), 1277-1288.

Hu, X., Rodgers, K., & Lovrich, N. P. (2018). "We are more than crime fighters": Social media images of police departments. *Police Quarterly*, *21*(4), 544-572.

Hu, X., & Lovrich, N. P. (2019). Social media and the police: A study of organizational characteristics associated with the use of social media. *Policing: An International Journal*, 42(4), 654-670

Kalemi, E., Yildirim-Yayilgan, S., Domnori, E., & Elezaj, O. (2017). SMONT: An ontology for crime solving through social media. *International Journal of Metadata, Semantics and Ontologies*, *12*(2-3), 71-81.

Kapoor, R., Kejriwal, M., & Szekely, P. (2017). Using contexts and constraints for improved geotagging of human trafficking webpages. In *Proceedings of the fourth international ACM workshop on managing and mining enriched geo-spatial data* (pp. 1-6).

Lavorgna, A., Middleton, S. E., Pickering, B., & Neumann, G. (2020). FloraGuard: Tackling the online illegal trade in endangered plants through a cross-disciplinary

ICT-enabled methodology. *Journal of Contemporary Criminal Justice*, *36*(3), 428-450.

Malleson, N., & Andresen, M. A. (2015). The impact of using social media data in crime rate calculations: Shifting hot spots and changing spatial patterns. *Cartography and Geographic Information Science*, *42*(2), 112-121.

Mateescu, A., Brunton, D., Rosenblat, A., Patton, D., Gold, Z., & Boyd, D. (2015). Social media surveillance and law enforcement. *Data Civ Rights*, *27*, 2015-2027.

Melekain, B. K., & Wexler, M. (2013). Social media and tactical considerations for law enforcement. *Office of Community Oriented Police Services*, from https://cops.usdoj.gov/RIC/Publications/cops-p261-pub.pdf

Nath, S. V. (2006). Crime pattern detection using data mining. In *2006 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology Workshops* (pp. 41-44). IEEE.

O'Connor, C. D. (2017). The police on Twitter: Image management, community building, and implications for policing in Canada. *Policing and Society*, *27*(8), 899-912.

O'Connor, C. D., & Zaidi, H. (2020). Communicating with purpose: Image work, social media, and policing. *The Police Journal*, 27(8), 899-912. 0032258X20932957.

Omand, D., Bartlett, J., & Miller, C. (2012). Introducing social media intelligence (SOCMINT). *Intelligence and National Security*, *27*(6), 801-823.

Patton, D. U., Brunton, D. W., Dixon, A., Miller, R. J., Leonard, P., & Hackman, R. (2017). Stop and frisk online: Theorizing everyday racism in digital policing in the use of social media for identification of criminal conduct and associations. *Social Media+ Society*, *3*(3), 1-10. 2056305117733344.

Piza, E. L., & Feng, S. Q. (2017). The current and potential role of crime analysts in evaluations of police interventions: Results from a survey of the International Association of Crime Analysts. *Police Quarterly*, *20*(4), 339-366.

Rønn, K. V., & Søe, S. O. (2019). Is social media intelligence private? Privacy in public and the nature of social media intelligence. *Intelligence and National Security*, *34*(3), 362-378.

Rovner, J. (2013). Intelligence in the Twitter age. *International Journal of Intelligence and Counterintelligence*, 26(2), 260-271.

Saldana, J. (2011). *Fundamentals of qualitative research*, (31-88). Oxford University Press.

Saldana, J. (2014). *Thinking qualitatively: Methods of mind*, (1-36). SAGE publications.

Saldaña, J. (2021). *The coding manual for qualitative researchers,* (4-17, 84-95). SAGE publications.

San Biagio, M., Acquaviva, R., Mazzonello, V., La Mattina, E., & Morreale, V. (2021, December). A new SOCMINT framework for Threat Intelligence Identification. In *2021 International Conference on Computational Science and Computational Intelligence (CSCI)* (pp. 692-697). IEEE.

Sanders, C., & Condon, C. (2017). Crime analysis and cognitive effects: The practice of policing through flows of data. *Global Crime*, *18*(3), 237-255.

Sathyadevan, S., Devan, M. S., & Gangadharan, S. S. (2014, August). Crime analysis and prediction using data mining. In *2014 First international conference on networks & soft computing (ICNSC2014)* (pp. 406-412). IEEE.

Scassa, T. (2017). Law enforcement in the age of big data and surveillance intermediaries: Transparency challenges. *SCRIPTed*, *14*, 239.

Shinta, O., & Logahan, J. M. (2019). Social media empowerment in implementing community policing: Study of the cybercrime investigation of the Indonesia national police. *UI Proceedings on Social Science and Humanities*, *3*(1).

Tracy, S. J. (2013). *Qualitative Research Methods*, (188-202). Wiley-Blackwell

Trottier, D. (2015). Open source intelligence, social media and law enforcement: Visions, constraints and critiques. *European Journal of Cultural Studies*, *18*(4-5), 530-547.

Walsh, J. P., & O'Connor, C. (2019). Social media and policing: A review of recent research. *Sociology compass*, *13*(1), e12648.

Williams, C. B., Fedorowicz, J., Kavanaugh, A., Mentzer, K., Thatcher, J. B., & Xu, J. (2018). Leveraging social media to achieve a community policing agenda. *Government Information Quarterly*, *35*(2), 210-222.

Wood, M. A. (2020). Policing's 'meme strategy': Understanding the rise of police social media engagement work. *Current Issues in Criminal Justice*, *32*(1), 40-58.

Zeng, D., Chen, H., Lusch, R., & Li, S. H. (2010). Social media analytics and intelligence. *IEEE Intelligent Systems*, *25*(6), 13-16.