Police Exploitation of Social Media for Information, Intelligence, and Investigation

Approved: *Dr. Cheryl Banachowski-Fuller*

Date: July 29, 2024

Police Exploitation of Social Media for Information, Intelligence, and Investigation

Seminar Paper Presented to The Graduate Faculty

University of Wisconsin-Platteville

In Partial Fulfillment of Requirements for the Degree

Master of Science in Criminal Justice

Steven E. Nusbaum

August 2024

Acknowledgments

It is seldom that we travel alone. Always with me, I am most thankful for my wonderful wife, Patty Ann McRae, my love, constant companion, source of inspiration, unwavering support, and foremost proofreader. I am grateful to Dr. Mohmmad El Bushra, a friend, colleague, and mentor. Thank you for setting me on this path. While my parents, regrettably, are unable to see the end of this journey, their contributions are immeasurable and deeply appreciated. I am also profoundly grateful to my sister Laura for her valuable assistance and support.

I thank the University of Wisconsin-Platteville faculty and staff, particularly Dr. Banachowski-Fuller and Dr. Hilal. Your guidance and support have been invaluable in keeping me on the path. I am also grateful to the State of Wisconsin and its Department of Veterans Affairs. Service is worth the price of admission.

Abstract

Communication is a crucial aspect of law enforcement, facilitating the exchange of vital information. As the latest form of communication, social media has become an integral part of this process. Given its novelty, the interaction between the law enforcement community and social media platforms must be clearly defined. This is because social media has evolved into a necessary element for the operation of police agencies. The best way to do this is by having clear and comprehensive policies and procedures. This study shows that many of the departments reviewed lack a practical social media policy or have no policy. This research paper thoroughly analyzes primary and secondary sources, including a systematic review, summary, and comparison of literature on collecting and using social media information. Additionally, the paper examines the ethical and legal considerations relating to collecting and using this information, emphasizing the importance of defining boundaries between public and privileged information, confidentiality, and consent. It reviews different policies and procedures various agencies use to effect decisions about acquiring and utilizing information from social media platforms. The result obtained serves as a reference to assist agencies in making policy decisions on regulating the obtaining and use of information from social media platforms. Equipped with this knowledge, departments and agencies can develop their policies and protocols, and maximize the use of social media platforms. The recommendations, if implemented, can potentially revolutionize the way law enforcement interacts with social media, ensuring a more ethical and effective use of these platforms.

Keywords: social media, law enforcement, policies, and procedures

Table of Contents

evidence. If carefully evaluated, these considerations can significantly shape local policies. It is important to note that management may not always adopt the recommendations in this research, but local factors should always be considered to develop the best plan.

Introduction

Statement of the Problem

Despite being relatively new, social media has become one of the leading communication entities. According to Dixon (2024), in 2023, social media platforms were used by almost 315 million people in the United States. Americans spend up to two and a half hours on social media daily (Ang, 2021). Social media platforms are interactive tools that facilitate communication. Information contained in social media, include user demographics, dialogues, notifications, videos, photos, and monologs. Recently, there have been growing concerns about social media, particularly regarding misinformation and privacy issues. Despite the potential benefits of utilizing information from social media platforms in investigations, it is not fully exploited. Omand et al. (2012) point out that police are not well equipped to collect and share intelligence information from social media platforms. This research shows that law enforcement would benefit from enhanced use of these platforms. Some law enforcement agencies have already realized the benefit of using social media as a tool to inform the public, request assistance, and collect information.

This research deals only with law enforcement collecting information from social media platforms. Since law enforcement's use of social media is relatively new, there are many issues related to collecting and using the data. The most recent survey by the International Association of Chiefs of Police and the Urban Institute reports that social media use proliferates among police departments (Kim et al., 2017). This increase can significantly impact police and policing in the United States. It presents a unique opportunity to incorporate social media into policing (Oh et al., 2021).

With increased social media use, issues arise regarding collecting and using information from these platforms. For this reason, litigation has been brought against numerous agencies. The Department of Homeland Security (DHS) (Levinson-Waldman & Guillermo Gutiérrez, 2023), The Washington DC Metro Police Department (Levinson-Waldman & Dyer, 2023), and the Minneapolis Police Department (Nelson & Sepic, 2023), are examples. Another issue is that electronic evidence can be problematic. Being relatively new, the courts have established stringent rules relating to the admissibility of electronic evidence. These and other issues can be effectively addressed by creating a "How to Manual" as a policy for managing information from social media. This research shows that not all agencies have social media policies, and few of the policies in use are complete. It emphasizes the importance of a comprehensive policy and details the elements of a good policy.

Gathering information is crucial to the efficient operation of law enforcement. It is a critical factor in solving crimes and impacts various activities, including daily operations, patrol activities, intelligence gathering, and investigations. This information can assist in strategic planning, contributing to such activities as patrol timing and location, developing leads, and providing evidence in investigations. Law enforcement's access to social media has the potential to play a significant role in police operations by obtaining more data in real-time. This research explores police interaction with social media to obtain intelligence information, information relative to investigations, evidence, and to conduct surveillance- "dataveillance" (Oconnor & Walsh, 2019). It also examines the "rules of engagement" when the information is exploited and the need for a comprehensive policy covering the rules.

Obtaining access to social media platforms can provide law enforcement agencies with significant information essential for maintaining safety and security in our communities. The

information obtained, however, must be governed by a comprehensive policy that ensures that the information is obtained legally and ethically.

Purpose of the Study

This research explores how police use social media to gather valuable and sometimes crucial information from social media posts. Social media platforms contain a vast amount of information about the community, individuals, and general and specific crimes. This includes personal information, demographics, photographs, narratives, monologue, dialogue, and video accounts. According to a recent survey, 59% of the agencies surveyed have contacted the social media platform to use information they obtained as evidence (Kim et al., 2017). Among the departments that use social media, 70% use it to gather intelligence (Kim et al., 2017). This research presents information about social media to understand what it is and how it is used to develop strategies to elicit information. Examining this information provides insight into how law enforcement can benefit from using social media to obtain information. Being aware of their presence and understanding the nature of the information offered on these platforms, along with how to utilize it effectively, is crucial to maximizing social media utility as a resource. As this information is collected and used, it is necessary to have a comprehensive policy to ensure the procedures are correct, legal, and ethical. This research presents policy considerations, best practices, and other policy considerations.

Significance of the Study

This paper argues for the increased utilization of social media platforms as a source of social media intelligence (SMINT). Despite the growing prevalence of social media in our daily lives, there is a lack of academic research on its use in criminal investigations, as highlighted by Rønn et al. (2020). Law enforcement agencies are constantly seeking new sources of information

to support their mission, and social media platforms offer a wealth of potential data. The value of this information to law enforcement cannot be overstated, with the vast number of social media users in the US spending nearly two and a half hours on these platforms each day, as Ang (2021) noted. As Falik et al. (2020) point out, social media platforms provide essential information for law enforcement in surveillance, intelligence gathering, and investigations. Policy guidance is necessary when gathering and using information from social media platforms. This research looks at the policies and procedures of various departments and documents relating to policy creation. Based on this information, guidelines and recommendations are suggested to improve operations and reduce liabilities.

Methods of Approach

A comprehensive analysis of primary and secondary sources was conducted with a systematic review, summation, classification, and comparison of pertinent literature. The sources of information utilized were comprised of peer-reviewed scientific articles and journals, government websites and documents, news articles, and program evaluations. Careful consideration was given to excerpts and relevant data from cited documentation to provide an insightful perspective that contributes towards a better understanding of social media platforms, the information they contain, the utilization of social media by law enforcement agencies, how to optimally leverage such information both legally and ethically.

Limitations

There is no one-size-fits-all approach to developing a social media policy. This research presents policy considerations with supporting evidence, comparing existing policies and presenting elements that make up a good policy. Management may not consider the

recommendations in this research to shape policy. As always, local factors must be evaluated to develop the best plan locally.

All the material for this research came from publicly accessible online sources. The information may have been changed or updated and not posted online. Additionally, not everyone is transparent. Some may have internal policy or verbal elements unavailable to the public. The Chicago Police Department exemplifies this (Chicago Police, 2020). There are also limits to the search queries made where not all the information is available. Related to this, some search returns were overwhelming, giving results too numerous to review. The research material is also limited by having no direct contact with the personnel involved in policy making or people working with the policy in the field.

When begun, this topic seemed limited in scope. The research revealed that it is much broader than expected. This presents an opportunity to research social media policy and procedure more thoroughly.

Contributions to the Field

This paper will demonstrate the need for law enforcement to collect information from social media platforms, consider the available information types, and explore various collection methods, focusing on best practices. Despite the potential benefits of using intelligence from social media platforms in investigations, it remains underutilized (Rønn et al., 2020). This research looks to bridge that gap and strengthen existing theories and models. It will present different policies and procedures various agencies use to inform policy decisions about acquiring and utilizing information from social media platforms. Moreover, the paper will examine the ethical and legal considerations surrounding the collection of such information, emphasizing the importance of defining boundaries between public and privileged information, confidentiality,

and consent (Omand et al., 2012). Given the vast volume of information and ease of access, establishing clear guidelines for collecting and using social media data is essential. This paper presents data and examples of policies and information that can be used to create a comprehensive social media policy.

Literature Review

Discussion of Information Available on the Platforms

The data available on social media varies depending on the platform. As an example, the platform Facebook help page lists the categories of information available:

- "Your Activity Across Facebook: Information and activity from different areas of Facebook, such as posts you've created, photos you're tagged in, groups you belong to and more.
- Personal Information: Information that you've provided when you set up your Facebook accounts and profiles.
- Connections: Who and how you've connected with people on Facebook, including things like your friends and followers.
- Logged Information: Information that Facebook logs about your activity, including things like your search history.
- Security and Login Information: Technical information and logged activity related to your account.
- Apps and Websites off of Facebook: Apps you own and activity we receive from apps and websites off of Facebook.
- Preferences: Actions you've taken to customize your experience on Facebook. • Ad information: Your interactions with ads and advertisers on Facebook" (Facebook, n.d.).

Social media platforms and the Internet have vast stores of information. The Supreme Court has recognized the Internet as, "the principal source for knowing current events, speaking and listening in the modern public square, and otherwise exploring the vast realms of human

thought and knowledge" — in other words, an essential means for taking part in public life and communicating with others. (Packingham v. North Carolina, 582 U.S. ___ (2017)).

These platforms can show all use, and the data available contains personal information, demographics, contacts, search data, connections, photographs, narratives, monologues, dialogues, and videos.

Approaches to Leveraging Information

Obtaining information from the Internet or a specific website such as social media is relatively easy if the information is public. The user may restrict, excepting the user ID, some or all of their information, removing it from the public domain. By creating a profile and logging on to the platform, all public information on the site is accessible. Most platforms have a search engine that returns results on a word, a phrase, or a name. This dedicated search engine allows a manual search of all profiles and public information. There are other means to get information on the Internet. Law enforcement uses data from the Internet as intelligence information and for evidence in an investigation. In the case of the Department of Homeland Security, persons were using aliases or fake identities to elicit information from others. The creation of fictitious profiles, including by law enforcement personnel, violates Facebook's policy (Levin & Bhuiyan, 2023). Although, it appears to be a continuing practice.

There are other means to obtain desired information from the Internet. Data mining searches the contents of a social media platform using specially developed software or algorithms, or in some cases, a company that specializes in data mining and analysis. This software allows the user to search the public information for specific data. Most programs then correlate the acquired data to meet specific pre-defined needs. In business, information on social media can be used to enhance a business's reputation and better understand users to improve

customer service and other things (Smith, 2024). Data mining can search all public information on the Internet or any individual website. Data mining can be accomplished using algorithms, specially designed software, or companies specializing in data mining. Rapid Miner is a commercially available software platform that uses text mining and predictive analysis (Xhafa & Schneider, 2022) (Altair® RapidMiner®, 2022). It may improve prediction and preemption of behaviors by helping law enforcement deploy resources more efficiently, ultimately aiding in crime prevention and interception and reducing crime rates (Oconnor & Walsh, 2019).

The anonymity offered by the Internet can be linked to criminality. (Edwards et al., 2015). Law enforcement agencies use social media data for investigative purposes, to detect threats, for situational awareness, and for immigration and travel screening (Levinson-Waldman et al., 2024). This is done using software designed to monitor social media to collect information. Omnivore and Carnivore are monitoring software used by the FBI in the 1990s. They are "packet sniffers" which target specific information. The agency collected information and monitored the activity of many individuals with Carnivore. The information collected from an Internet provider includes all online activity, not just social media (Frey & Cruz-Cruz). Now, agencies seldom have the resources to conduct monitoring, so they often contract with private companies. Media monitoring can include tracking all information generated at the user's Internet Protocol (IP) address or monitoring traffic to a specific website. This monitoring can seek general or definitive data from users (Singh, 2023). Examples of entities that contract for monitoring services include SS8 (Kozbielak & Stimson, 2023), Dataminr (2024), and Atis Digital (Digital, 2022). Some platforms have limited the choice of a source for data mining. Facebook, in 2021, banned seven surveillance companies (Bond, 2021). However, anyone can monitor or intercept data with sufficient resources and the correct software or programming.

Information Retrieval: Open Access and Restricted Information

The social media platforms differ in rules about who can access the site and how much user profile is visible to the public (Howard, 2008). The user may also restrict, excepting the user ID, some or all of their information. By creating a profile and logging on to the specific platform, all public information on the site is accessible. Most platforms also have a search engine that returns results on a word, a phrase, or a name. This dedicated search engine allows a manual search of all public information. Data mining searches the contents of a social media platform using specially developed software. This software allows the user to search public information for specific data. Most programs then correlate the acquired data to meet specific needs. A business can use the information on social media to enhance its reputation and gain a better understanding of users to improve customer service and other things (Smith, 2024).

When law enforcement agencies deal with information, it is essential to distinguish between public and private information. Public information is data easily retrievable by anyone without restrictions, while private information restricts those persons or groups allowed access by the owner or by legal process. Moreover, the Constitution's Fourth Amendment protects private information on the Internet from unlawful search and seizure.

Accessing and Using Information from Social Media Platforms

Law enforcement deals with two types of data when monitoring or obtaining information from the Internet: public and private. Public information is data accessible by anyone without any expectation of privacy. The definition used by the U.S. government is:

- Printed or broadcast information meant for public use,
- Any information that the public can request,
- Information accessed by the public online or otherwise.

- Information obtained by purchase or with a subscription,
- The information available at a meeting or other event open to the public (Authentic8, 2019).

Private information has restrictions, and there is a reasonable expectation of privacy. This information should not be available to the general public but only to those with permission to access the data. Permission is discussed in the section on legal considerations below.

Law enforcement agencies use social media data for investigative purposes, to detect threats, to develop situational awareness, and for immigration and travel screening (Levinson-Waldman et al., 2024). They do this through the use of monitoring services, software, or programming designed to intercept, analyze, and collect information or data.

Legal and Ethical Considerations When Accessing and Using Information from Social Media Platforms

The rapid emergence of social media and the Internet and its use by law enforcement agencies has resulted in the lack of clear guidelines regulating their use. Trottier (2015) discusses the issues of obtaining and using this data with concerns about a lack of clear legal and procedural protocols. These issues have led to the filing of numerous court cases seeking clarification on the collection and use of information. These lawsuits include those seeking the release of information (Levinson-Waldman & Dyer, 2023), the reformation of police monitoring (Levinson-Waldman & Diaz, 2020), and disclosure of tools used to collect and analyze data (Levinson-Waldman & Guillermo Gutiérrez, 2023). After receiving an unsatisfactory response from DHS, the Brennen Center filed a lawsuit against DHS seeking the same information (Levinson-Waldman & Guillermo Gutiérrez, 2023), (Levinson-Waldman et al., 2022). The tools in question relate to the company “Shadow Dragon” and its software “Socialnet”, (*SocialNet - investigate social networks, profiles, links and activity* 2024). The software can give law

enforcement access to data from social media and about 120 other Internet locations, including the ”dark net” and sites claiming to be end-to-end encrypted (Kwet, 2021).

Personal information and personal identifying information (PPI) appearing on the Internet and social media platforms are subject to some regulatory protection. As mentioned earlier, a social media poster may have a reasonable expectation of privacy. The problem becomes, are public posts on social media platforms really public? Since the person posting the data believes that only permitted people will access the data, does the poster have a reasonable expectation of privacy (Bousquet, 2016)? Existing principles offer limited guidance on accessing and using Internet data. This guidance includes the First Amendment protecting speech, the Fourth Amendment protecting from unlawful search and seizure, and the Fourteenth Amendment protecting various groups of people (Levinson-Waldman et al., 2024). There are also some individual agency regulations relating to data collection and use. Data collection and use legislation includes 5 U.S. Code § 552a - Records maintained on individuals (5 U.S. Code § 552A - records maintained on individuals). Law enforcement must be aware of these privacy protections when accessing data on the internet.

This issue becomes especially true when the court considers the data presented to support a case in court. The second U.S. Circuit Court recognized the problems of dealing with the law on evidence acquired from the Internet by saying that applying traditional law to the complexities of the Internet is analogous to attempting to board a moving bus (Bensusan Restaurant Corp. v. King, 126 F.3d 25). In addition to evidentiary issues, accessing personal information and other data from the Internet presents ethical issues.

For example, the ACLU (2016) complains that anyone who speaks out against the government receives the label of a terrorist in social media surveillance. During an investigation

of the Minneapolis police department, the Minnesota Department of Human Rights found that the department practiced racial discrimination. This investigation included social media surveillance (MPD investigation findings, 2024). The New York City Police Department also received allegations of racism in social media surveillance (Patton et al., 2017). Hence, collecting information using intrusive methods for social media surveillance must have a legitimate reason, especially when it may violate some privacy issues (Liviu et al., 1970).

In other words, by establishing a transparent, inclusive policy that regulates activity and addresses legal and privacy concerns, ethical and legal issues encountered in the use of social media can be eliminated or substantially reduced (Liviu et al., 1970).

Literature Review Conclusion

Based on the information in the literature review, evidence supports that creating a clear and comprehensive policy for social media interaction relating to investigations and intelligence gathering is a vital tool for all law enforcement agencies. This tool should include developing policies and procedures, designating a dedicated worksite, allocating resources, and training personnel. The literature also shows that law enforcement is open to legal action and loss of investigatory evidence without a good policy. The research also suggests the usefulness of the development of a universal policy. However, given that different jurisdictions have diverse needs, this universal policy could serve as a baseline that each department can adjust to fit the requirements of each department.

Program Evaluation

Introduction

The interaction between law enforcement and the Internet has been evolving over the past decade. A comprehensive policy governing the interaction between law enforcement and social media platforms is essential to prevent complications arising or becoming more convoluted. Although at times contentious, this relationship has been a learning process shaped by interaction with other law enforcement agencies, Internet contacts, litigation, and information released through channels such as the Freedom of Information Act (FOIA). Consequently, both sides have, through experience, developed rules governing this interaction. This research examines and compares policies used by various departments and agencies to collect intelligence and evidence from social media platforms. Information regarding social media policies for this research comes primarily from online sources.

History

Social media is a complex term that is challenging to define due to its complexity. According to Kaplan and Haenlein (2010), social media is "a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of User Generated Content." In other words, websites developed the capacity and allowed users to create an account from which they can exchange information with other account holders. These websites began to emerge in the late 1990s. Boyd & Ellison (2007) identified the first social media website as Six Degrees.com, which started in 1997. They chart the beginning and evolution of social media websites. For example, their chart shows that the creation of Facebook in 2004 was initially limited to Harvard University. In 2005, Facebook expanded to high school networks, and in 2006, Facebook was released to corporate networks

and eventually made available to the public that year. Social media sites have expanded and now contain an extraordinary amount of information. This information can be invaluable to law enforcement.

Use of Social Media Platforms by Law Enforcement

Although this research deals with using social media to obtain data for investigation and intelligence purposes, the police have other operations on these platforms. Using social media platforms to gather investigatory and intelligence information does not play a primary role in law enforcement's Internet use. Boston, Massachusetts, police department, for example, used social media with significant effect in communicating with the community following the Boston Marathon bombings (Davis et al., 2014). A survey of law enforcement use of social media conducted in 2016 by the International Association of Chiefs of Police and the Urban Institute shows that out of ten applications of police activity, intelligence gathering for investigations is seventh (Mohr et al., 2017). The sixth most used category surveyed is monitoring public sentiment, which is classified under intelligence as situational awareness for this research. The remaining uses for social media by law enforcement relate to interaction with the community. Of the departments surveyed, 72% reported using social media platforms to monitor public sentiment, and 70% reported using these platforms for gathering intelligence in investigations. About 80% have a policy dealing with social media. According to the survey, 59% of the departments surveyed have contacted social media platforms to obtain and preserve evidence.

Law enforcement can use social media platforms to access such information. The data revealed on these platforms can assist an investigator, be evidence, or be the basis for an online case. Identification can be made with facial recognition software. A determination of situational awareness can be acquired. Using these platforms, predictive policing is possible. Social media

platforms require a comprehensive policy to ensure that all data is legally obtained, used, and stored and has a proper disposition.

Policy Considerations

After reviewing the social media policies of various agencies, it is evident there are both commonalities and significant differences in the topics and content addressed by these policies. A review of various police social media policies was completed for comparison. Moreover, data suggests the components of these policies and provides guidance on creating a policy. Also examined was information on the impacts of social media policies, or the lack thereof, both negative and positive. This information includes the Internet and other media sites praising a department's use of social media to help the department and the community. The review includes data related to transparency, information on police social media policies, and Freedom of Information Act (FOIA) requests. It also covers litigation brought against law enforcement agencies over their social media policies. The analysis examines general topics on social media, including general information, the history of social media to gather data relating to the policies of social media platforms, the interaction of law enforcement with the platforms, and the use of social media by police agencies.

The data review reveals that there are more than a few issues with the interaction of law enforcement and social media platforms. Too many departments lack a comprehensive social media policy addressing investigatory and intelligence gathering or have no policy at all. The Brennen Center for Justice conducted a nationwide analysis of available law enforcement social media policies and stated they “have serious deficiencies” and that those “can lead to grave consequences” (Levinson-Waldman & Gutiérrez, 2024). When departments lack a robust policy, it can create or complicate encounters by police when using social media.

Generating an excellent social media policy can be challenging because departments have varied needs and use the Internet differently. A needs assessment may be extremely helpful in constructing a social media policy. Agencies must recognize that existing policies related to internet usage, electronic communication, codes of conduct, and media relations may address potential issues (NCJRS Virtual Library 2019). The Internet is also in constant flux, so policy considerations need to change or be modified, corresponding to the evolving landscape encountered on the Internet and social media platforms.

Upon review, it is evident that there is a considerable lack of comprehensive policies for social media investigations and intelligence gathering. As a result, it is necessary to make amendments or completely restructure the policy (Levinson-Waldman & Gutiérrez, 2024).

Transparency

In an article on transparency, accountability, and constitutional policing, the US Conference of Mayors (2020) stated that police reform will not happen solely through training and improved policies. That, however, is a strong beginning. Concerns have been raised about the lack of transparency in law enforcement's social media policies on collecting and using information (Levinson-Waldman & Gutiérrez, 2024). Transparency is critical for reducing negative feelings and issues relating to law enforcement's use of social media and other Internet sources. Posting policies, such as social media policies, on department websites increases transparency and, thus, public trust by letting the public know what the department is doing. It also makes the department and its employees more accountable to the community, primarily through Freedom of Information Requests (FOIA).

Legal and Ethical Considerations

There are other issues to consider when preparing a policy. For instance, the department must ensure the elements of the policy are legal (*Social Media - International Association of Chiefs of Police* 2019), (*Liverman v. City of Petersburg, 844 F.3d 400, 409 (4th Cir. 2016)*), where the court found that the social media policy of The Petersburg, Virginia Police Department violated the First Amendment. After the 9-11 attacks in New York, the U.S. District Court revised the 1985 guidelines for dealing with the investigation of political activities (*Handschu v. Special Services Division, 71-cv-2203 (CSH) (S.D.N.Y.)* 2006). The delineation of political and criminal is critical to any data recovery. Before use, a determination must be made whether there is a legitimate law enforcement purpose for data collection and whether the information is relevant and necessary for the performance of the activity (Levinson-Waldman, 2024).

As previously mentioned, litigation has been brought against numerous agencies, including the Department of Homeland Security (DHS), seeking disclosure of information resulting in a lawsuit attempting to identify which tools DHS was using to monitor data (Levinson-Waldman & Guillermo Gutiérrez, 2023). The Washington DC Metro Police Department is being sued for their records on social media surveillance (Levinson-Waldman & Dyer, 2023), and the Minneapolis Police Department is being sued by the National Association for the Advancement of Colored People (NAACP) regarding covert surveillance by police (Nelson & Sepic, 2023). Privacy and free speech are foundational rights in American society. These rights must be ensured in any data collection conducted on the Internet.

Training is crucial regarding the legal and ethical considerations of social media policy. Issues relating to statutory, case, and Constitutional law must all be considered. Given the recent rise of social media, few legal aspects of the legal system have been applied to its use by the

government. It is necessary to proceed cautiously to protect the officers, the department, the community, and the rights of the individuals and organizations involved. This lack of clear direction has led to unfortunate occurrences such as criminal and civil litigation. To avoid legal issues, a policy must be clear and comprehensive. Contacting the legal section to review the proposed activity is always advisable to ensure it is lawful at the start. The Chicago Police Department has developed a presentation that covers the topic in detail and gives many examples for study (Chicago Police Department, 2020), ensuring that officers are prepared and competent in this area.

Wording documentation for social media activities is also critical. Surveilling activist groups such as Black Lives Matter (BLM) may be a violation of the First Amendment. Surveilling the activity rather than the group may make a difference (Villasenor et al., 2020).

Exploiting social media and the Internet must be used only for a valid law enforcement purpose. It must not target individuals or organizations solely based on their religious, political, or social views or activities or an individual's race, ethnicity, citizenship, place of origin, disability, gender, or sexual orientation (Madison, WI Police Department, 2024).

Evidence

Again, digital evidence collection, use, and sharing are critical to include in any social media policy. Keeping this element current regarding legislation and court rulings is vital. If an error is made related to laws and constitutional rights, even inadvertently, it may result in a lost case or civil or criminal litigation against the department or the employee. The Bureau of Justice Assistance, (2022) awarded funding to develop a Digital Evidence Management and Integration Project to form a basis for policymaking for digital evidence. Shorr et al. (2023) have done a series of podcasts related to digital evidence. Their content concerns collecting and maintaining

digital evidence to ensure its validity and acceptance in legal proceedings. Jackson et al. (2015) prepared a paper identifying technology and other things necessary to collect and use digital evidence. This paper presents an early view of electronic evidence issues, many of which remain the same. Furthermore, it discusses the need to educate people involved in collecting and preserving digital evidence. When using digital evidence in legal proceedings, the prosecution must determine relevance under the Federal Rules of Evidence (Sozio, 2017). Once the evidence is determined relevant, the evidence must receive authentication.

Information must be evaluated to determine confidence levels (source reliability and content validity) (Bureau of Justice Assistance, 2013). Authenticating internet data can be challenging. Some sites, such as government websites, are self-authenticating. Examining others can present prima facie evidence, aiding in the authentication of data (Joseph, 2022). Examining all digital evidence acquired aids in establishing source reliability and content validity, assisting with validating the evidence. Policy considerations relating to digital evidence may be training and the isolation and security of areas and equipment for data collection.

Authorization and Control

Another significant aspect to consider in developing a policy is authorization and control. To ensure a digital operation is necessary and relevant, it must be the responsibility of the person in authority to clear it. Typically, this person would be the head of the department or his designee. Furthermore, supervision of the operation is necessary to ensure the operation is progressing within the boundaries of the policy. Depending on the department's resources, this person may be the case supervisor, the head of intelligence, or the head of the technical staff.

Equipment Use and Duty Status

The definition of activity on and off duty and using personal and department resources is also essential. Performing casework off duty and using personally owned equipment outside of an emergent situation may create difficulty. Using designated equipment in a controlled environment under proper supervision leads to fewer errors and ensures the proper acquisition and storage of evidence.

Documentation

It is important to develop rules for documentation. These rules must address the collected data's storage, use, sharing, and disposition. Information can be documented in case files and logs. 28 CFR 23.20 (g)(2) (2024), the federal government’s operating policies for criminal intelligence systems establish several policies relative to this. It sets conditions for the retention, storage, dissemination, and disposition of collected information.

Analysis

Another element to consider is the establishment of rules for analysis. Who analyzes the data collected, and how is the analysis conducted? Are the results repeatable? In other words, will the analysis yield the same result each time? Is a person or departmental-approved software doing the analysis?

Undercover Accounts

Control of undercover accounts is critical. In the past, officers or departments established undercover accounts to gain information. The account holder poses as someone he is not to elicit specific information from social media sites. In some jurisdictions, this is not an issue and has been used effectively to identify and arrest child predators. These accounts and the individuals using them must be required to obtain supervisory approval, legal documentation such as search warrants if required, and careful review and documentation. If an actual person is being impersonated, none of the personal information or the password should be changed, and the person being impersonated must be allowed to terminate participation at any time (Levinson-Waldman, 2024).

Data Mining and Surveillance Operations

Careful consideration must be taken when using software, algorithms, and companies designed to monitor, extract, and analyze data. These tools are effective for gathering information that is invaluable to law enforcement. However, by their very nature, it is easy to mistakenly gather irrelevant information, otherwise restricted data, or information that is out of context. Exploiting social media and the Internet must be used only for a valid law enforcement purpose. It must not target individuals or organizations solely based on their religious, political,

or social views or activities or an individual's race, ethnicity, citizenship, place of origin, disability, gender, or sexual orientation (Madison, WI Police Department, 2024).

The government's monitoring of social media can lead to negative consequences. These include the wrongful implication of criminal activity by persons or groups based on their social media data, misinterpretation of the meaning of information gathered from social media data, suppression of communication due to fear, and the invasion of privacy through the data collection (Levinson-Waldman et al., 2024). Some algorithms, software, monitoring tools, and contracting firms that monitor Internet activity collect a large amount of data and can store it indefinitely. *Shadow Dragon* claims it has "archive datasets going back many years" (*SocialNet - investigate social networks, profiles, links and activity* 2024). *Babel Street* is used by several federal government agencies, including DHS and the Federal Bureau of Investigation (FBI) (Dwyer et al., 2021). *Bable Street* claims it accesses over three billion Internet sites and processes 200 million documents daily in more than 200 languages (Bowen et al. - *Threat Intelligence Tool*). *Bable Street* claims to be "An award-winning platform" and is praised by David P. Glaser, the former Provost Marshal General of the Army (Bowen et al. - *Threat Intelligence Tool*). The collection of this information can have a significant impact on public safety and officer well-being. Much of the data collection and analysis of data is done by Artificial Intelligence (AI). Boolean search terms used in an AI platform, such as "Muslim extremist, search on both words individually and together. The word Muslim can return a huge range of data; however, very few Muslims are related to terrorism. Muslim, Arab, Middle Eastern, and South Asian communities are often singled out by the screening criteria (Levinson-Waldman et al., 2024). Two examples of the data miners' failure to perform as expected relate to the "underwear bomber" and the "Fort Hood shootings" by Major Nidal Hasan. The failure was

due to the overwhelming amount of information presented by the search (Levinson-Waldman, 2013). The Fort Hood data showed no adverse information and did not predict the event until after the incident occurred. Data collection that can be unrelated to the desired information is often unintentional. It is often the fault of AI to collect and analyze the data accurately. The sheer volume of data is often so large that human vetting is impractical.

The use of these tools has harmed social media platforms as well. In her article for National Public Radio, Bond (2021) reports that the parent company of the social media platform Facebook banned seven "surveillance for hire" companies, claiming they had spied on 50,000 Facebook users. Facebook claimed these companies were trying to fool users into disclosing personal information. Some of the platforms involved are *Pegasus, Black Cube, Servicefacebook. Bluehawk CI, ProQuest,* and others, some of which are related to China. Although none of these operations are known to be used by law enforcement agencies in the U.S., it follows that some of the algorithms, software, and companies engaged in monitoring activities for the police may be using the same method of operation. In December 2021, the U.S. Congress requested sanctioning the NSO Group, a surveillance company, and others for enabling human rights abuses (Bond, 2021).

Data mining tools such as GeoFeedia were able to gain comprehensive access to "backend data streams" (Bousquet, 2016). The term' backend' encompasses all data processing within the app, including message sending, login verification, news feeds, updates, data storage, and more (Keblas & Didenko, 2024). This level of access means that the tool had the potential to collect all data on the platform, not just the public information, raising significant privacy concerns.

In January 2015, the head of the Oregon Department of Justice (DOJ) Civil Rights Division was targeted by the tool Digital Stakeout used by the Oregon DOJ. The target was identified through his tweet about a group of musicians, “Public Enemy,” because of search terms used in the surveillance. The data gathered by the program was misinterpreted, and investigations ensued. The initial investigation was of the target, based on the results reported by the surveillance software. A subsequent investigation examined the officer pursuing the first case (Sepulvado, 2020).

Police use these tools to gather information, which coincides with “Predictive Policing.” Predictive policing involves using data to predict where and when problems may occur. With this technology, law enforcement can, in theory, form a good idea of where and when problems will occur. This would make the police proactive rather than reactive (Pearsall, 2010), (Perry et al., 2013).

Before any algorithms or software are used or contracted with a data collection or analysis company, a comprehensive product analysis must be conducted. This step is crucial to guarantee that the product aligns with the department's standards and will produce the desired result. The use of such tools must also be approved at the upper levels of the department. While law enforcement agencies often use social media tools to gather crucial information and evidence, many departments have faced challenges with these tools. Hundreds of agencies lack the necessary safeguards to prevent officers from misusing social media to target First Amendment activity and minorities (Levinson-Waldman & Gutiérrez, 2024).

Obtaining and retaining information through social media sites can be complex. The most popular social media platform, Facebook, now known as Meta, posts a large amount of information on several web pages relating to the interface between them and law enforcement

(Law enforcement guidelines: Meta safety center n.d.). Meta Platforms, Inc. only discloses account records in compliance with our terms of service and applicable law, including the federal Stored Communications Act ("SCA"), 18 U.S.C. Sections 2701-2712. In some cases, judicial subpoenas are required. In other instances, a warrant is demanded. This ensures that the privacy of individuals is respected and that the information is obtained legally. To require disclosure of certain information about the account, a court order issued under 18 U.S.C. Section 2703(d) is required (Meta, n.d.). For Meta, the request process begins with the web page Facebook, Law Enforcement Online Requests (n.d.). For queries that involve evidence, a request must be submitted to preserve the account (Meta, n.d.) so the digital evidence can be retained, authenticated, and presented in a legal proceeding. The reliability and content validity of the data must be ensured, as with any other investigation. Information from social media can be valuable, but it requires thorough evaluation for reliability and proper caveats (Bureau of Justice Assistance, n.d.). There is also access to other platforms, such as Twitter, now X (X, n.d.).

Separation of Activities

Another critical aspect of a good policy is separating Internet operations from other activities. Ideally, these operations should be carried out in a designated secure room accessible only to authorized personnel. The equipment used for intelligence and investigatory purposes should be supplied by the department and used solely for a single operation. Therefore, each operation needs its own workstation and equipment. This will ensure that the desired results are obtained while maintaining high standards, making it easier to authenticate evidence and maintain the evidence's chain of custody. Additionally, using personally owned equipment should be discouraged due to the potential risks of data security breaches and the difficulty in authenticating evidence obtained from such equipment. Work on the operation should be done

during work time to ensure the integrity of evidence and other data. 28 CFR 23.20 (g)(2) (2024), the federal government's operating policies for criminal intelligence systems present several policies relative to the isolation and security of equipment and facilities used.

Training

Some of the primary challenges agencies encounter when using social media include adapting to new trends, assessing the impact of their use of technology, and training personnel to utilize social media effectively (Mohr et al., 2017). Few of the policies reviewed included training as a part of their policy. Although the Internet is not new, it is a recent phenomenon. Many people have little or no knowledge about the online world. It is essential to train continuously on current issues, the risks associated with social media, and self-protection (Waters, 2012). With the lack of proper training, there is a risk of losing the case or exposing the officer and the department to civil and criminal liability.

Section 341.8 of the Green Bay Policy Manual regarding the use of social media states: "Authorized members should receive training that, at a minimum, addresses legal issues concerning the appropriate use of social media sites, as well as privacy, civil rights, dissemination and retention of information posted on department sites" (Green Bay Police Department, 2024). Not included in Chicago Police's social media policy is an instruction from its Bureau of Counterterrorism directing training for investigations and intelligence gathering (Chicago Police Department, 2020).

There are many sources for training in this area. Training in this field is offered to departments and officers at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia (FLETC, n.d.). Online training is available through sources such as Blue Force Learning: *https://www.blueforcelearning.com/courses*. Several courses are offered online

relating to 28 CFR Part 23: *https://28cfr.ncirc.gov/Login*. This includes implementing standards for operating federally funded, multijurisdictional criminal intelligence systems. It applies to systems operating through federal funding under Title I of the Omnibus Crime Control and Safe Streets Act of 1968, as amended. Colleges and community colleges offer courses that offer a better understanding of computers, the Internet, software, and other related things. Some of these courses are offered online. An additional resource is the department IT office and other officers who are experienced users. Kahn Academy offers courses in computer and Internet topics free of charge (Kahn Academy, n.d.).

Social media platforms are not going away soon. Surveillance of these platforms can provide law enforcement agencies with critical information, offering a promising tool for the future. Collecting intelligence data for situational awareness and data related to investigations appears to be a relatively good tool. It can analyze trends, media, and population sentiment and integrate cameras into its predictions where available. This can be useful for public events, disasters, and other emergencies (Kelly, 2022). It can also be helpful to get leads and obtain evidence to support investigations.

The nature of data on the Internet is dynamic, making it challenging to develop a policy with complete coverage. Case precedents and legislation also change the operation of police Internet interaction. Therefore, each topic must be considered to determine its application to the use of social media (Oglesby-Neal & Warnberg, 2019). This requires continuous monitoring of the legal aspects relating to social media policymaking to ensure the policies are current.

Review of Current Policies

Levinson-Waldman (2020) provides a directory of police department social media policies by state and city. The National Sheriff's Association outlines the social media policy of

twenty-four departments in its Policy Examples and Considerations (National Sheriffs' Association, *LESM: Policy examples and considerations,* n.d.). Some links to the policies are broken and attempts to obtain the information by other means are ineffective. Many policies reviewed do not address using social media for investigation or intelligence. For example, the Pasco WA County Sheriff's Office policy spans twenty-six pages and does not mention investigation or intelligence even once (*Pasco Sheriff's Office Social Media Plan* (n.d.). Levinson-Waldman and Gutiérrez (2024) examined the social media policies of 328 police departments. They found that only 162 departments had the policy posted on their website. This leaves, perhaps, two hundred departments without a social media policy. They also found that although many policies mentioned using social media platforms for investigation, only seventy-four contained specific details on how the data would be obtained or used. No single policy has been encountered that demonstrates best practices in all areas.

Elements Presented for Consideration in Law Enforcement Social Media Policies

Sources reviewed recommend general elements included in a law enforcement social media policy. Police1 (2010) presents policies currently in use as examples. NeoGov (2022) presents elements that include the use of social media. The Bureau of Justice Statistics (2013) lists the key elements of a social media policy as:

I. State that the use of social media resources will comply with applicable laws, regulations, and other agency policies,

II. Define when the use of social media sites or tools is authorized and how the information is to be used,

III. Establish the authorization levels needed for each activity,

IV. Address evaluation to establish source reliability and content validity,

V. Specify storage and retention requirements for information obtained,

VI. Require reasons and purpose for use by off-duty personnel and the use of personal equipment,

VII. Dictate dissemination procedures for criminal intelligence and investigative data, including personally identifiable information (PII).

The Author recommends the addition of these elements to any policy:

VIII. Designation of exclusive use areas,

IX. Training of personnel.

The following is a brief of social media policies in select U.S. cities. The social media policy information was obtained from internet sources. Criteria used for review are based partly on elements from the Levinson-Waldman (2024) website. This review samples the policies of several major departments and agencies. The following chart details how the policies examined correspond to the criteria suggested by Levinson-Waldman in the Directory of Police Department Social Media Policies (2024):

- Contemplated uses for social media (other than public-facing use) and requirements for use in investigations,
- Prohibitions on the use of social media,
- Specific rules for situational awareness or other non-investigative efforts,
- Authorization required for general use,
- Limitations on undercover/covert activity,
- Language governing the use of personal devices or accounts,
- Retention and storage of information and procedures for electronic evidence,
- Discussion of constitutional rights.

See Appendix A for a detailed comparison of the social media policies reflected in Chart 1.

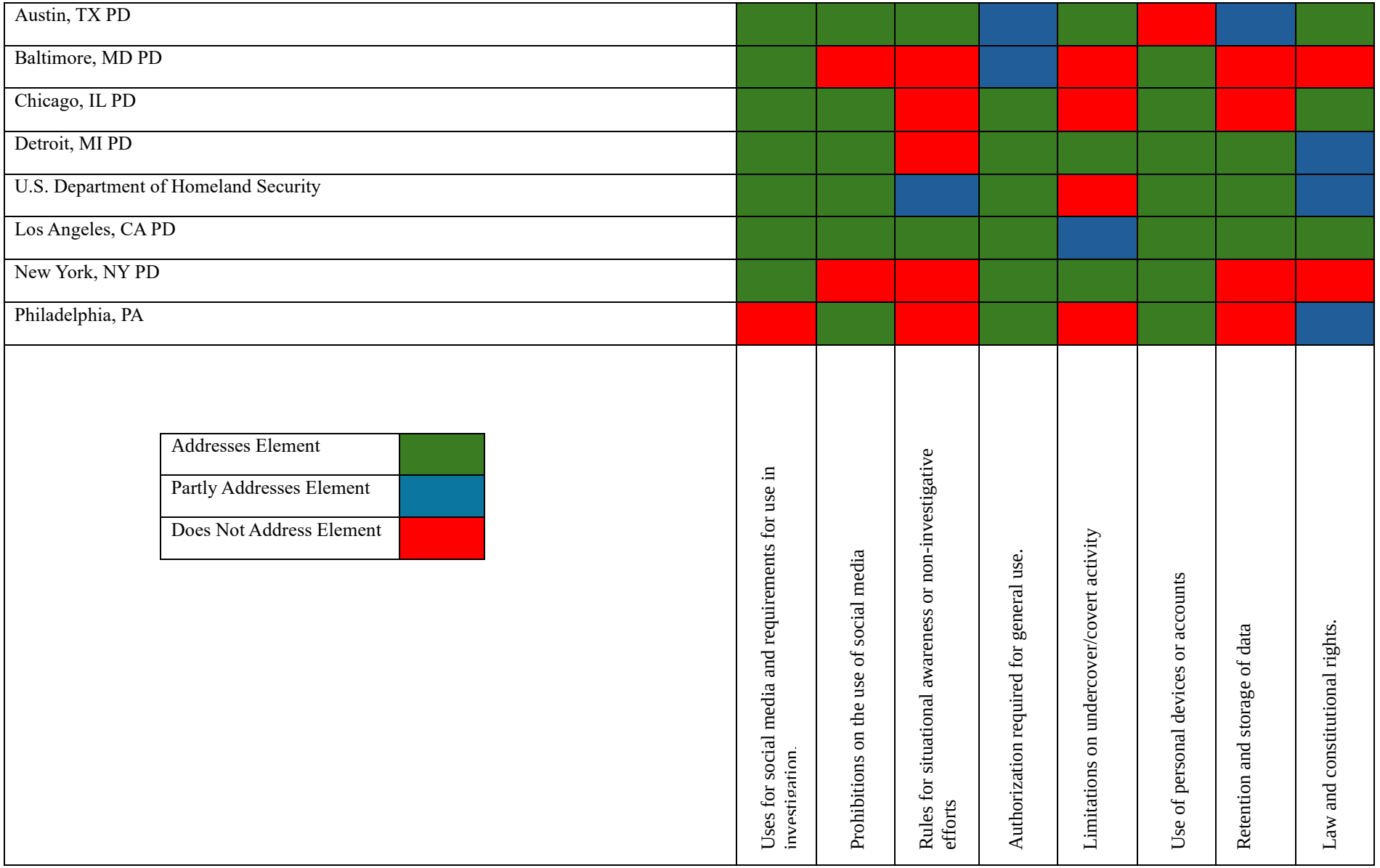

Chart 1, Policy Element Comparisons by Department

The information below summarizes the Austin, Texas social media policy elements, Austin Police Department General Orders (2021), using the Levinson-Waldman (2024) criteria. The elements are displayed in Chart 1. Summaries for other reviews of the exact nature can be found in Appendix A.

Austin, TX Police Department

Austin Police Department General Orders (2021)

- **Contemplated uses for social media (other than public-facing use) and requirements for use in investigations:**
  The policy provides that social media may be used only for a "valid law enforcement purpose," which includes "crime analysis and situational assessment reports; criminal intelligence development; or criminal investigations." The policy goes on to say that police department employees may only "seek or retain" information on social media when the information is "based on a criminal predicate or threat to public safety, is relevant to the investigation and prosecution of suspected criminal incidents, resulting justice system response, enforcement of sanctions, orders, or sentences, or the prevention of crime; or is useful in crime analysis or situational assessment reports for administration of criminal justice and public safety." The policy also permits the use of social media when there is "reasonable suspicion that an identifiable individual or organization" is engaged in criminal conduct or poses a threat to others and the information to be obtained from social media is "relevant to the criminal conduct or activity." The policy directs officers to evaluate social media for reliability and validity.

- **Prohibitions on the use of social media:**
  - The policy prohibits using social media to "seek or retain information" about individuals or organizations based on various protected categories. These include religion, political association, social views or activities, race, ethnicity, citizenship, place of origin, disability, gender, or sexual orientation (except for the categories from race through sexual orientation, where those characteristics are "relevant to individual's criminal conduct or activity" or are needed for identification). Social media also may not be used to collect or retain information about an "individual's participation in particular non-criminal organization or lawful event," or about an individual's age, unless to determine if the person is a minor.

- **Specific rules for situational awareness or other non-investigative efforts:**
  - Crime analysis and situational assessment reports may be used for "special events management, including First Amendment-protected activities." Social media information must be deleted within 14 days if there is no related criminal activity.

- **Authorization required for general uses:**
  - No authorization is required for "general research, topical information, or other law enforcement uses" if those uses do not require an online alias.

- **Limitations on undercover/covert activity:**
  - Use of an online alias requires a criminal predicate or threat to public safety or reasonable suspicion that an identifiable individual or organization has committed a crime or is involved in or is planning criminal conduct or activity that presents a threat to an individual, the community, or the nation, and the information is relevant to the criminal conduct or activity.

  - Employees must get approval from their supervisor to use an online alias based on evaluating whether an online alias would serve a valid law enforcement purpose. The policy establishes a specific approval process and requires deconfliction through the local fusion center (the Austin Regional Intelligence Center). All approved undercover activity requests must be reviewed at least every 90 days by a supervisor and will be discontinued if the activity does not provide information regarding a valid law enforcement purpose. Employees with an approved online alias can use it to "make false representations in concealment of personal identity in order to establish social media accounts."

  - The policy specifies that "online undercover activity" entails interaction with an individual online, not simply surveillance. Employees may only undertake online undercover operations "when there is reason to believe that criminal offenses have been, will be, or are being committed (e.g., internet chat rooms where child exploitation occurs)."

- **Language governing use of personal devices or accounts:**
  - The policy does not contain language regulating department employees' use of personal devices or accounts to access social media data.

  - **Discussion of constitutional rights:**
    The policy states that the Austin Police Department "will not seek or retain information about individuals or organizations solely based on their religion, political association, social views or activities [or an] individual's participation in a particular non-criminal organization or lawful event." The policy states that the department will not use social media to seek or

retain information on an individual based on their protected characteristics unless they are "relevant to the individual's criminal conduct or activity or if required to identify the individual."

- The policy allows officers to use social media monitoring tools to prepare crime analysis and situational awareness reports for special events, including First Amendment-protected activities. However, if there was no criminal activity, information about an event obtained through the social media monitoring tool will not be retained for more than 14 days.

The policies reviewed and the material covered in the discussion of police social media policymaking are detailed further in the next section.

Recommendations

"To successfully and lawfully harness the power and value of social media sites while ensuring that individuals' and groups' privacy, civil rights, and civil liberties are protected, agency leadership should support the development of a policy within their agency regarding the use of social media sites in criminal intelligence and investigative activity" (Bureau of Justice Assistance, 2013).

This review revealed that numerous agencies do not have a policy related to law enforcement interaction with social media platforms when conducting investigations and gathering intelligence. Many departments with a social media policy do not address social media use for investigatory or intelligence purposes. Chicago has two policies. One is for public dissemination. The other is a confidential "not to be disclosed outside the department" policy (Tirado, 2020). The public accessible policy has accreditation from CALEA® | The Commission on Accreditation for Law Enforcement Agencies, Inc. (Chicago Police Department, 2020), (CALEA, 2024). It is important to remember that some departments may have other policies that cover the use of social media for investigation and intelligence but are not credited as social media policies. Additionally, the Chicago Police Confidential Analytics Section—Bureau of

Counterterrorism has prepared a presentation on social media investigation policies. This presentation not only explains the CPD's policy but gives numerous examples relating to the policy and other issues such as law and the Constitution (Chicago Police Department, 2020)

A policy is beneficial in many ways. By clearly defining procedures, it protects privacy and civil liberties. It can offer guidance on using social media platforms to collect valuable data. A policy must give clear guidance, definitions, and rules and assign responsibility for managing and overseeing online operations (Eidam, 2021). This can increase transparency and is necessary for accountability. Policies establish standards for acquiring, using, storing, and disposing of social media data and safeguarding information and evidence. Legal and ethical considerations should also be included in a good social media policy, reducing the risk of legal challenges and damage to reputation. Finally, a good policy that the department's needs are met effectively and ethically.

Not every agency can adopt the same social media policy. The policy should be tailored to each agency's specific needs, ensuring that each agency's unique challenges and opportunities are considered. All policies should reflect the same principles used in all law enforcement. Actions taken during data collection and agency interaction with social media must have a clearly defined objective and a valid purpose (Developing a policy on the use of social media - bureau of justice ... n.d.). 28 CFR 23.20 (g)(2) (2024), Criminal Intelligence Systems Operating Policies offers federal rules for collection, use, and dissemination of intelligence information. Many of the rules can cover Internet data used in investigations as well. Law enforcement social media policies must be publicly available, providing transparency and outlining practices, restrictions, and oversight requirements, ensuring that the public and stakeholders are informed and confident in the agency's operations (Levinson-Waldman, 2024).

Additionally, many social media platforms have developed rules for interaction with law enforcement regarding legal issues (Law enforcement guidelines: Meta safety center, n.d.).These rules must be followed to preserve evidence because the information can be compromised or lost at any time. The process of seeking information, authentication, and account preservation are all covered in detail.

After analyzing numerous law enforcement social media policies and related material describing the development of social media policies, the following suggests components and analysis for compiling a comprehensive social media policy. Segments of current social media policies are included and referenced.

A. Purpose

This element is important because it clearly states under what circumstances the department can use social media platforms. This can be simply for investigating where leads and evidence can be obtained from social media platforms. It could also be an intelligence operation to research an upcoming event to determine the deployment of resources to ensure proper coverage.

This portion should address the specific circumstances and conditions under which the Internet and social media platforms can be used in an official context to carry out investigations and gather intelligence information. There must be a clear justification for using the Internet for an investigation or intelligence operation, and the nexus and relevancy between criminal activity and the threat to public safety must be identified. Additional details that should be considered include: Can the department access social media photos for facial recognition, which is questionable in some jurisdictions?

Sample Purpose Statement

> This policy establishes guidelines for using Internet-based social media platforms to gather intelligence, conduct investigations, and conduct research(Bureau of Justice Assistance, n.d.).

> Social media can allow access to data relating to gang activity, online crimes, photos or videos depicting criminal activity, and crime prevention. It may also be utilized for crime and information analysis, situational assessment reports, criminal intelligence development, and criminal investigations. This policy establishes standards of conduct for using the Internet and similar technologies for investigative purposes (Madison, WI PD, 2024).

B. Definitions

Definitions become essential because they clarify the meaning of specific terms used extensively on the Internet. Some of the terms related to the Internet may be unfamiliar to some of the people assigned to collect data from social media platforms. A policy can have as many definitions as needed, and additional terms can be added as they appear. There is no numerical requirement for definitions.

Sample Definitions

- Social Media Platform- an interactive technology that enables users to create content, share it, and participate in social networking (Obar & Wildman, 2015)
- Public Domain Data is a data category not protected by intellectual property law. It is free for anyone to use, adapt, reproduce, or distribute (Volle, n.d.) In the case of social media, the data refers to information that the data's owner has not restricted.
- Exigent Circumstances refer to situations of extreme urgency where there is no time to obtain a legal process, such as a warrant, which would normally be required (Justia Legal Dictionary, n.d.).
- Blog- A website that displays self-published posts containing comments, videos, and photos by one or more persons. The posts are usually in reverse chronological order, and there are often links to comments on the specific postings (Merriam-Webster, n.d.).

- Web Page- consists of a group of files that form a document when displayed by a web browser. A web page can contain text, graphics, and links to other pages and files (Computer Hope, 2023).

- Post- a social media post is a message published on a platform. The content can vary, including text, images, video, and audio files (SocialBee, 2024).

- Browser- a tool that allows access to websites. The website's address can be entered directly, or the browser can search for the information given, which presents a list of possibilities.

- Profile- a dataset of personal information users enter onto a social media platform. The profile can contain identifying information and often includes a photograph identifying the person posting.

- Speech- expression or communication of thoughts in various means, spoken words, writing, body language, symbols, photographs, video, or related forms of communication (Bureau of Justice Assistance, n.d.).

- Electronic Communications- refer to the transfer of data by electronic means. This includes email, instant messaging, texting, chat rooms, and social media platforms (Proofpoint, 2023).

- Crime Analysis and Situational Assessment Reports- —Analytics for identifying, understanding, and predicting trends, causes, and potential signs of criminal activity, including terrorism.

- Criminal Intelligence Information- refers to information gathered, analyzed, and/or shared to predict, prevent, or monitor criminal activities conducted by individuals or organizations reasonably suspected of involvement in criminal activities (IACP, 2021).

- Criminal Nexus- the connection of criminal activity to an individual or organization.

- Social Media Monitoring Tool-algorithms, software, or an entity contracted to monitor Internet or social media activities for law enforcement purposes.

- Valid Law Enforcement Purpose- is the same for electronic use as it is for other police operations. "Valid law enforcement purpose" refers to a purpose that involves developing or collecting information for the authorized functions and activities of a law enforcement agency. This may involve preventing crime, ensuring public safety, protecting public and private property, enhancing officer safety, and contributing to homeland and national security while upholding the laws and policies safeguarding Americans' rights and civil liberties. (Bureau of Justice Assistance, n.d.).

- Online Surveillance- the following of a person, persons, or group's activity online.
- Fictitious Online Persona- a false identity or alias created for use online. It can also be adopting an actual profile to obtain information about that person.
- Classified Information- any information with a legal national security designation of confidential or higher.

C. Authorization Required for the Use of Social Media

Authorization takes place at different levels depending on the level of engagement. Apparent or overt access is looking at public information by using a search engine to search for information or to locate a name or address on a public Facebook page, for example, locating a city council member or searching general information. When the use becomes more discreet, higher authority is required. This would be engaged if the searches became limited to specific individuals or groups where the information is retained for future reference. Covert use begins when an alias account is set up and the account friends or follows the target being considered. This also includes lawful intercepts and surveillance. The department must define the activities at various levels and then assign the appropriate level of supervision to authorize the action (Bureau of Justice Assistance, 2013). Accountability is vital in all police activities. Overall, it is always good advice to document everything to cover your assets (CYA) (Anderson, 2021). Documentation belongs in a case file or a case log. If a search warrant is required, there are samples on the Internet to use as a model (Computer Crime and Intellectual Property Section (CCIPS), 2009).

Sample Authorization Statement

Authorization For the use of Social Media for Investigative and Intelligence Purposes

Authorized Users

- Only personnel authorized by the agency director or his designee may use social media platforms and other Internet resources in an official capacity.

Requesting Authorization

- All requests for official use of social media or other Internet resources for investigative or intelligence operations will be routed through the supervisory chain of command to the director for approval. The request will contain information regarding the target(s) of the operation, identify a valid law enforcement purpose, the reason for the operation, why the use of the Internet is necessary, any nexus to criminal or terrorist activity, how the operation will obtain information, such as through searches or surveillance, any tools to be used for collection or analysis of the information, and the anticipated duration and outcome of the operation. As the level of engagement increases, the level of authorizing officials must also increase (Bureau of Justice Assistance, 2013).

Monitoring of Operations

- The immediate supervisor in charge of the operation must submit a written report of its activities to the director every month it is conducted. Every six months, the next highest supervisor will audit the operation.

Online Profile

- Requesting authorization for an online profile or alias is the same as requesting authorization for an Internet operation. The request will document the necessity for the profile or the alias.

Authorization for the use of Online Surveillance Tools

- Requests For real-time online surveillance or analysis tools will be routed through the supervisory chain of command to the director for approval. The request will additionally contain a precise reason the tool(s) is necessary, the data to be retrieved by the tool(s), and the level of information to be examined, whether public or protected. All legal requirements will be met and documented. Tools will be closely monitored and considered for termination if issues warrant the action.

D. Use of Department Equipment and Personal Devices

The federal government's intelligence community recognizes the need to restrict the use of personal devices and software for official work. In its operating policy for criminal intelligence systems, the project must restrict access to its facilities, operating environment, and documentation to organizations and personnel authorized by the project (28 CFR 23.20 (g) (2), 2024). To ensure the integrity of the operation, an isolated operating environment must be created accessible only to authorized persons. The equipment used, likewise, must be for use by the project only. Different projects and users would have individual, logged access to dedicated equipment. The use of non-departmental owned and controlled equipment is prohibited. Software, Local Area Networks (LAN), Internet Service Providers (ISP), all connections, and Virtual Private Networks (VPN) must also be accessed through the department. Since all activities are conducted at a location and with equipment dedicated to the operation, they will be conducted while on duty. These principles are also reflected in the Chicago Police Department general order G09-01-06 (2023).

Sample Use Policy

Equipment Use for an Online Operation

- Only authorized department-owned equipment will be used for approved Internet or social media operations. No non-department-owned equipment, software, or connections will be used for these operations (Cruz, 2023).
- The dedicated equipment for online operations will be kept in the "online operations room," which will be accessible only to those persons authorized by the operation.
- All equipment with Internet access will require a separate login for each person using it.

- The IT department will establish all connections, provide required hardware and software, and use precautionary measures such as a Virtual Private Network (VPN).

E. Documentation, Dissemination, and Retention

Developing a policy relating to case documentation for collecting electronic information should be comparable to other department policies relating to regular investigations or intelligence operations (Bureau of Justice Assistance, 2013). In its operating policy for criminal intelligence systems, the federal government dictates that criminal intelligence information will be disseminated only to law enforcement authorities who have agreed to follow procedures outlined in the policy (28 CFR 23.20 (g)(2), 2024).

This policy also includes instructions on the retention and destruction of information. Information to be retained must be relevant and vital, and unreliable or obsolete information must be reviewed for destruction.

Chicago Police Department general order G09-01-06 (2023), in subsection X, addresses the “Reporting and Disseminating” of a social media investigation. This section requires written reports on a special report form, distribution to supervision, and retention in specific files. Distribution outside the department requires a documented official request approved by supervision.

Sample Policy Statement for Documentation, Dissemination, and Retention

- All personnel initiating a social media investigation will complete the appropriate criminal or non-criminal case report, documenting information and intelligence received via social media sites. Completed reports will be submitted to a supervisor for approval. Upon approval, original reports will be retained in the proper file corresponding to the request. Copies of the original reports will be disseminated to a unit supervisor, to which the intelligence relates, for inclusion in the official case file.

- Reports will not be distributed outside the Department unless a request is made in writing and approved by the supervisor. Electronic criminal intelligence information will report the contents of stored electronic messages, such as emails, which contain content applicable to investigative or intelligence activity. These retained electronic communications will be incorporated into case documents for court discovery purposes. If information cannot be printed due to the short duration of the information being available (e.g., Snapchat). Any information of investigatory value will be documented in an investigatory report (IACP, 2019).

- All reports generated under this directive will be retained under existing department retention directives and existing record preservation orders.

Legal and Ethical Considerations

Ensuring that social media content complies with relevant laws, regulations, and policies is crucial. This includes adhering to information technology and records management policies and respecting content, ideas, and materials protected by law, such as copyright, trademark, service mark restrictions, and public records laws (IACP, 2019). Trottier (2015) discusses the challenges of obtaining and using data, mainly due to the lack of clear legal and procedural protocols. These issues have resulted in numerous court cases being filed to seek clarification on the collection and usage of information. Exploiting social media and the Internet must be used only for a valid law enforcement purpose. It must not target individuals or organizations solely based on their religious, political, or social views or activities or an individual's race, ethnicity, citizenship, place of origin, disability, gender, or sexual orientation (Madison, WI Police Department, 2024).

F. Evidence

Evidence collected from the Internet is a realistic method to enhance legal proceedings. This evidence supports both Internet cases and other cases not related to the Internet. According to a recent survey, 59% of the agencies surveyed have contacted the social media platform to use

information they obtained as evidence (Kim et al., 2017). The introduction of electronic evidence into the legal system has presented potential difficulties in two areas. Since it is recent, electronic evidence has not been tested by other legal elements. Almost every case sets new precedent. This evolving case law requires constant policy changes and updates. The second problem is the lack of knowledge of the Court, especially prosecutors (Jackson et al., 2015). Electronic evidence on social media must be "preserved by the platform. This is done at the department's request since the material can be easily removed at any time (Chicago PD, 2020), (Facebook, *Law Enforcement Online Requests* n.d.). Most departments have a well-developed evidence policy to which they can refer. evidence (*LAPD: 2022 Digital Evidence Management and Integration Project* 2022). General policies such as Property & Evidence Control published by the IACP (2021) are available. There are not sufficient resources to outline and evidence policy in this research.

Training is crucial regarding a social media policy's legal and ethical considerations. Issues relating to statutory, case, and Constitutional law must all be considered. Given the recent rise of social media, few aspects of the legal system have been applied to its use by the government, either by statute or case law. It is necessary to proceed cautiously to protect the employees, the department, the community, and the rights of the individuals and organizations involved. This lack of clear direction has led to unfortunate occurrences such as criminal and civil litigation. To avoid legal issues, a policy must be clear and comprehensive. Contacting the legal section to review the proposed activity is always advisable to ensure it is lawful at the start. The Chicago Police Department has developed a presentation that covers the topic in detail and gives many examples for study (Chicago Police Department, 2020), ensuring that officers are prepared and competent in this area.

When using information as evidence, assessing its reliability and confidence level is crucial (source reliability and content validity) (Bureau of Justice Assistance, 2013).

G. Training

Section 341.8 of the Green Bay Policy Manual regarding the use of social media states: "Authorized members should receive training that, at a minimum, addresses legal issues concerning the appropriate use of social media sites, as well as privacy, civil rights, dissemination and retention of information posted on department sites" (Green Bay Police Department, 2024). Not included in Chicago Police's social media policy is an instruction from its Bureau of Counterterrorism directing training for investigations and intelligence gathering (Chicago Police Department, 2020).

All staff participating in the agency's social media program should receive initial and ongoing training. This training should reinforce existing agency policies and guidelines related to social media while allowing employees to learn about emerging social media technology and contemporary best practices. Networking with peers and sharing best practices should be encouraged for all staff (IACP, 2019).

There are many sources for training in this area. Training in this field is offered to departments and officers at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia (FLETC, n.d.). Online training is available through sources such as Blue Force Learning: *https://www.blueforcelearning.com/courses*. Several courses are offered online relating to 28 CFR Part 23: *https://28cfr.ncirc.gov/Login*. It contains implementing standards for operating federally funded, multijurisdictional criminal intelligence systems. It applies to systems operating through federal funding under Title I of the Omnibus Crime Control and Safe Streets Act of 1968, as amended. Colleges and community colleges offer courses that offer a

better understanding of computers, the Internet, software, and other related things. Some of these courses are offered online. An additional resource is the department IT office and other officers who are experienced users. Kahn Academy offers courses in computer and Internet topics free of charge (Kahn Academy, n.d.).

Sample Training Statement

- All personnel using social media or other Internet platforms must be proficient in using electronic devices and other hardware and software necessary to engage with investigation or intelligence information. The department will meet identified training needs. Individuals involved in these operations are encouraged to expand their knowledge in the field by obtaining additional training individually.

H. Review

As with all policies, a social media policy needs constant review (Oglesby-Neal & Warnberg, 2019). This is especially true given the rapidly changing Internet landscape.

Sample Review Statement

- This social media policy will be reviewed and appropriately revised at least every six months or more often if necessary to keep it current.

Conclusion

Clearly, social media and the Internet offer a wealth of real-time information about almost any subject. Law enforcement must take advantage of that information to help ensure safety and stability. There are many ways to retrieve data from social media platforms, such as a simple search, a targeted search, or surveillance. It is critical that law enforcement know the proper manner in which to obtain, use, disseminate, and dispose of the data. To do this, law enforcement must implement a comprehensive policy to govern social media and Internet data collection and use. The Bureau of Justice Assistance (2013) agrees that the successful exploitation of social media sites while protecting privacy, civil rights, and civil liberties must be supported by the development of a policy regarding the use of social media for investigative and

intelligence activity. An inclusive social media policy benefits law enforcement and the public (Parkin & Rice, 2016). It provides guidance in the new and primarily uncharted territory of social media and the Internet and the methods to obtain information from these platforms. It also directs law enforcement to adhere to the high standards of behavior for collecting and using the data, ensuring ethical and legal practices are adhered to. A proper social media policy will ensure the data is appropriately handled, protecting privacy rights and public safety.

References:

ACLU. (2016, September 22). *Police use of social media surveillance software is escalating, and activists are in the digital...* Medium. https://medium.com/@ACLU_NorCal/police-use-of-social-media-surveillance-software-is-escalating-and-activists-are-in-the-digital-d29d8f89c48

American Civil Liberties Union. (2015, September 2). *DEA Handbook: Online Investigative Principles for Federal Law Enforcement Agents*. American Civil Liberties Union. https://www.aclu.org/documents/dea-handbook-online-investigative-principles-federal-law-enforcement-agents

Anderson, I. (2021, August 6). *Cya – meaning, origin, usage*. DigitalCultures. https://digitalcultures.net/abbreviations/cya/

Altiar. (n.d.). *Altair® RapidMiner®*. Altair RapidMiner. https://altair.com/altair-rapidminer

Ang, C. (2021, December 10). *Ranked: The world's most popular social networks, and who owns them*. Visual Capitalist. https://www.visualcapitalist.com/ranked-social-networks-worldwide-by-users/

AUTHENTIC8. (2019, October 23). *Publicly available information: Risks, benefits, and "why there needs to be a change."* Federal News Network.

Baltimore Police Department. (2016, July 1). *Social Media*. Baltimore Police Department. https://www.baltimorepolice.org/transparency/bpd-policies/604-social-media

Beck, C. (2015). Los Angeles police department social media users guide. Retrieved from https://ia801000.us.archive.org/15/items/LosAngelesPoliceDepartmentSocialMediaPolicies/2015_03_12_lapd_chief_charlie_beck_lapd_social_media_guide_OCOP_Notice_03-12-2015.pdf

BlueForce Learning. (n.d.). *Law enforcement training: Online courses: Blue force learning*. https://www.blueforcelearning.com/courses

Bond, S. (2021, December 16). *Facebook bans 7 "surveillance-for-hire" companies that spied on 50,000 users*. NPR. https://www.npr.org/2021/12/16/1064628654/facebook-bans-surveillance-firms-that-spied-on-50000-people

Bousquet , C. (2016, April 26). *Mining social media data for policing, the ethical way*. Mining Social Media Data for Policing, the Ethical Way. https://datasmart.hks.harvard.edu/news/article/mining-social-media-data-policing-ethical-way Bowen, E. (Ed.). (n.d.). *Data Analytics Platform - Threat Intelligence Tool*. Babel Street. https://www.babelstreet.com/

Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. Journal of Computer-Mediated Communication, 13(1), 210–230. https://doi.org/10.1111/j.1083-6101.2007.00393.x

Bureau of Justice Assistance. (2013, February). *Developing a policy on the use of social media*. Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities Guidance and Recommendations. https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/developing_a_policy_on_the_use_of_social_media_in_intelligence_and_inves.pdf

Bureau of Justice Assistance. (n.d.). Tips and leads and threats to life. https://bja.ojp.gov/promising-practices.pdf

CALEA | The Commission on Accreditation for Law Enforcement Agencies, Inc. (2024). *Accreditation programs*. Accreditation Programs | CALEA® | The Commission on Accreditation for Law Enforcement Agencies, Inc. https://www.calea.org/accreditation-programs

Callahan, M. E. (2012, June 8). *PRIVACY POLICY FOR OPERATIONAL USE OF SOCIAL MEDIA*. DHS Instruction Number: 110-01-001.

https://www.dhs.gov/sites/default/files/publications/Instruction_110-01-001_Privacy_Policy_for_Operational_Use_of_Social_Media_0.pdf

Chicago Police Department. (2020, February 5). Policy Review posts. *Social Media Policy Draft*. https://home.chicagopolice.org/draft_policy/social-media-policy-draft/

Chicago Police, American Civil Liberties Union. (2020). Confidential Analytics Section Social Media Investigations Policies, Part 1. https://www.aclu-il.org/sites/default/files/cpd_cas_training_socail_media_investigations_2020-compressed.pdf

Chicago Police Department. (2023, January 13). *Chicago Police Department general order G09-01-06 use of social media ...* Use Of Social Media Outlets. https://home.chicagopolice.org/wp-content/uploads/G09-01-06_Use-of-Social-Media-Outlets_DRAFT-For-Posting_13JAN23.pdf

City of Detroit. (2020, January 23). Department internet usage/web pages / social networking – 102.8. https://detroitmi.gov/document/department-internet-usage-web-pages-social-networking-1028

City of Madison, WI Police. (2024, January 23). *Social Media - investigative use*. City Of Madison Police Department Standard Operating Procedure. https://www.cityofmadison.com/police/documents/sop/SocialMediaInvestUse.pdf

Computer Hope. (2023, September 12). *What is a web page?* Computer Hope. https://www.computerhope.com/jargon/w/webpage.htm

Cruz, R. (2023, July 10). *The power and danger of social media for law enforcement*. Route Fifty. https://www.route-fifty.com/management/2020/07/the-power-and-danger-of-social-media-for-law-enforcement/315140/

Davis, E. F., Sklansky, D. A., & Alves, A. A. (2014). NCJRS Virtual Library. Social Media and Police Leadership: Lessons From Boston | Office of Justice Programs. https://www.ojp.gov/ncjrs/virtual-library/abstracts/social-media-and-police-leadership-lessons-boston

Digital, A. (2022, August 3). *Lawful interception software solutions, digital logging recorder, Legal Monitoring Solutions*. atis. https://www.atisdigital.com/product/network-based-lawful-interception/

Dwyer, M. P., Gutiérrez, J. G., Levinson-Waldman, R., Dyson, I., Ayoub, E., Jaloza, S., Goitein, E., & Toh, A. (2021, December 15). *Third-party vendors of social media monitoring tools for Law Enforcement Agencies*. Brennan Center for Justice. https://www.brennancenter.org/our-work/research-reports/third-party-vendors-social-media-monitoring-tools-law-enforcement

Dixon, S. J. (2024, May 22). *Biggest social media platforms 2024*. Statista. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

Dixon, S. J. (2024, January 30). *U.S.: Social media users 2020-2029*. Statista. https://www.statista.com/statistics/278409/number-of-social-network-users-in-the-united-states/

Eidam, E. (2021, April 23). *4 factors agencies should consider when developing a social media policy*. GovTech. https://www.govtech.com/gov-experience/4-factors-agencies-should-consider-when-developing-a-social-media-policy.html

Edwards, M., Rashid, A., & Rayson, P. (2015). A systematic survey of online data mining technology intended for law enforcement. *ACM Computing Surveys*, *48*(1), 1–54. https://doi.org/10.1145/2811403

Facebook. (n.d.). *Law Enforcement Online Requests*. Facebook. https://www.facebook.com/records/login/

Fallik, S., Deuchar, R., Crichlow, V., & Hodges, H. (2020). Policing through social media: A qualitative exploration. *International Journal of Police Science & Management*, *22*, 146135572091194. https://doi.org/10.1177/1461355720911948

Federal Law Enforcement Training Center. (n.d.). *Internet investigations training program*. Go to Federal Law Enforcement Training Centers Producer Resource Steward seal. https://www.fletc.gov/internet-investigations-training-program

Frey, W. J., & Cruz-Cruz, J. A. (2005). (dissertation). *Privacy and Surveillance: The Carnivore case*. Retrieved June 6, 2024, from chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://computingcases.org/adobe_files/Additional.Cases/Carnivore.pdf.

Global Top Sites. Amazon Alexa. (n.d.). http://www.alexa.com/site/ds/top_sites?ts_mode=global&lang=none

Gottfried, J. (2024, January 31). *Americans' social media use*. Pew Research Center. https://www.pewresearch.org/internet/2024/01/31/americans-social-media-use/

Green Bay Police Department. (2024, March 12). *Green Bay Police Department - Policy Manual*. Green Bay Police Department - Policy Manual | Green Bay, WI. https://greenbaywi.gov/1223/Policy-Manual

Handschu v. Special Services Division, 71-cv-2203 (CSH) (S.D.N.Y.) (https://casetext.com/case/handschu-v-special-services-division June 20, 2006).

Hernandez v. City of Phoenix, 541 F. Supp. 3d 996 (D. Ariz. 2021) (9th Circuit May 26, 2021).

Howard, B. (2008). Analyzing online social networks. *Communications of the ACM*, *51*(11), 14–16. https://doi.org/10.1145/1400214.1400220

IACP Law Enforcement Policy Center. (2021, July). *Criminal intelligence*. Criminal Intelligence. https://www.theiacp.org/sites/default/files/2021-08/Criminal%20Intelligence%2008.2021.pdf

International Chiefs of Chiefs of Police (IACP) Law Enforcement Policy Center. (2019, May). *Social Media - International Association of Chiefs of Police*. Concepts & Issues Paper Social Media. https://www.theiacp.org/sites/default/files/2019-05/Social%20Media%20Paper%20-%202019.pdf

International Association of Chiefs of Police. (2019). *NCJRS Virtual Library*. Social Media: Concepts and Issues Paper | Office of Justice Programs. https://www.ojp.gov/ncjrs/virtual-library/abstracts/social-media-concepts-and-issues-paper

Jackson, B. A., Davis, R. C., & Goodison, S. E. (2015, April 20). *Digital Evidence and the U.S. Criminal Justice System*. Priority Criminal Justice Needs Initiative. https://www.ojp.gov/pdffiles1/nij/grants/248770.pdf

Joseph, G. P. (2022, July 27). *What every judge and lawyer needs to know about electronic evidence*. Judicature. https://judicature.duke.edu/articles/what-every-judge-and-lawyer-needs-to-know-about-electronic-evidence/

Justia Legal Dictionary. (n.d.). *Exigent circumstances*. Dictionary. https://dictionary.justia.com/exigent-circumstances

Khan Academy. (n.d.). *Computing*. Khan Academy. https://www.khanacademy.org/computing

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! the challenges and opportunities of social media. Business Horizons, 53(1), 59–68. https://doi.org/10.1016/j.bushor.2009.09.003

Kim, K., Oglesby-Neal, A., & Mohr, E. (2017, February). *2016 law enforcement use of Social Media Survey*. 2016 Law Enforcement Use of Social Media Survey. https://www.urban.org/sites/default/files/publication/88661/2016-law-enforcement-use-of-social-media-survey.pdf

Kietzmann, J. H., Hermkens, K., McCarthy, I. P., & Silvestre, B. S. (1970, January 1). *Social Media? get serious! understanding the functional building blocks of social media*. Business Horizons. https://summit.sfu.ca/item/18103

Kozbielak, M., & Stimson, S. (2023, October 4). *Check out SS8's latest lawful intelligence insights*. SS8 Deploys Leading Lawful Interception Solutions in Public Cloud. https://www.ss8.com/ss8-deploys-leading-lawful-interception-solutions/

Kwet, M. published in C. L. N. D. (2021, November 15). *ShadowDragon: Inside the Social Media Surveillance Software That Can Watch Your Every Move | Criminal Legal News*. Criminal Legal News. https://www.criminallegalnews.org/news/2021/nov/15/shadowdragon-inside-social-media-surveillance-software-can-watch-your-every-move/

Law enforcement guidelines: Meta safety center. Meta. (n.d.). https://about.meta.com/actions/safety/audiences/law/guidelines

Learn what categories of information are available in your Facebook settings: Facebook help center. Learn what categories of information are available in your Facebook settings | Facebook Help Center. (n.d.). https://www.facebook.com/help/405183566203254/

Legal Information Institute. (n.d.). *5 U.S. Code § 552A - records maintained on individuals*. Legal Information Institute. https://www.law.cornell.edu/uscode/text/5/552a

Levin, S., & Bhuiyan, J. (2023, September 5). *Revealed: How US immigration uses fake social media profiles across investigations*. The Guardian. https://www.theguardian.com/us-news/2023/sep/05/us-immigration-homeland-security-social-media-fake-profiles

Levinson-Waldman, R. (2020, July 9). *Directory of police department social media policies*. Directory of Police Department Social Media Policies. https://www.brennancenter.org/our-work/research-reports/directory-police-department-social-media-policies

Levinson-Waldman, R., & Dyer, M. P. (2023, December 12). *We're suing DC Police for records on social media surveillance*. Brennan Center for Justice. https://www.brennancenter.org/our-work/analysis-opinion/were-suing-dc-police-records-social-media-surveillance

Levinson-Waldman, Rachel, Gutiérrez, J. G., Panduranga, H., Pablo, E. M., Dyson, I., Milner, Y., Griffiths, H., Snow, J., Reynolds, S., & Patel, F. (2022a, August 18). *Brennan Center Files Freedom of Information Act requests for information on DHS's use of social media monitoring tools*. Brennan Center for Justice. https://www.brennancenter.org/our-work/research-reports/brennan-center-files-freedom-information-act-requests-information-dhss

Levinson-Waldman, Rachel. (2013, June 7). *The real problem with data mining*. Brennan Center for Justice. https://www.brennancenter.org/our-work/analysis-opinion/real-problem-data-mining

Levinson-Waldman, Rachel, & Guillermo Gutiérrez, J. (2023, December 12). *We're suing DHS to uncover its use of social media surveillance tools*. Brennan Center for Justice. https://www.brennancenter.org/our-work/analysis-opinion/were-suing-dhs-uncover-its-use-social-media-surveillance-tools

Levinson-Waldman, Rachel. (2024b, February 7). *Principles for social media use by law enforcement*. Brennan Center for Justice. https://www.brennancenter.org/our-work/research-reports/principles-social-media-use-law-enforcement

Levinson-Waldman, R., Panduranga, H., & Patel, F. (2024, May 15). Social media surveillance by the U.S. Government. https://www.brennancenter.org/our-work/research-reports/social-media-surveillance-us-government

Levinson-Waldman, R, & Gutiérrez, J. G. (2024, February 7). *Study reveals inadequacy of police departments' social media surveillance policies*. Brennan Center for Justice. https://www.brennancenter.org/our-work/analysis-opinion/study-reveals-inadequacy-police-departments-social-media-surveillance

Liviu , A., Nicolae, M., Codruta, R., & Anamaria, C. (1970, January 1). *Social Media Intelligence: Opportunities and limitations*. CES Working Papers. https://ideas.repec.org/a/jes/wpaper/y2015v7i2ap505-510.html

Liverman v. City of Petersburg, 844 F.3d 400, 409 (4th Cir. 2016) (https://casetext.com/case/liverman-v-city-of-petersburg-5 December 15, 2016).

Los Angeles, CA Police Department. (2015, March 12). *Notice March 12, 2015 14.5 to: All Department personnel from: Chief of ...* LAPD - Social Media User Guide. https://ia801000.us.archive.org/15/items/LosAngelesPoliceDepartmentSocialMediaPolicies/2015_03_12_lapd_chief_charlie_beck_lapd_social_media_guide_OCOP_Notice_03-12-2015.pdf

Maryville University. (2024, April 24). *The evolution of social media: How did it begin, and where could it go next?* Maryville University Online. https://online.maryville.edu/blog/evolution-social-media/

McCartney, S., & Parent, R. (2015, April 17). *4.3 the Milgram experiment*. Ethics in Law Enforcement. https://opentextbc.ca/ethicsinlawenforcement/chapter/the-milgram-experiment/

Minnesota Department of Human Rights. (2024, February 5). *MPD investigation findings*. Minnesota.gov. https://mn.gov/mdhr/mpd/findings/

media surveillance by cops. MPR News. https://www.mprnews.org/story/2023/04/26/naacp-sues-city-of-minneapolis-over-covert-social-media-surveillance

Merriam-Webster. (n.d.). *Blog definition & meaning*. Merriam-Webster. https://www.merriam-webster.com/dictionary/blog

National Sheriff's Association. (n.d.). *LESM: Policy examples and considerations*. LESM: Policy Examples and Considerations | National Sheriffs' Association. https://www.sheriffs.org/lesm/policy

Nelson, T., & Sepic, M. (2023, April 27). *NAACP sues Minneapolis, alleging covert social media surveillance by cops*. MPR News. https://www.mprnews.org/story/2023/04/26/naacp-sues-city-of-minneapolis-over-covert-social-media-surveillance

NeoGov. (2022, December 22). *Law Enforcement Social Media Policy*. PowerDMS. https://www.powerdms.com/policy-learning-center/law-enforcement-social-media-policy

New York City Police Department. (2012, May 9). Use of Social Networks for Investigative Purposes-General Procedure. https://s3.documentcloud.org/documents/1507881/responsive-documents.pdf

Obar, J. A., & Wildman, S. S. (2015, August 26). *Social Media Definition and the governance challenge: An introduction to the special issue*. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2647377

Oconnor, C., & Walsh, J. (2019). *Social Media and Policing: A review of recent research*. Social media and policing: A review of recent research. https://www.researchgate.net/publication/328817058_Social_media_and_policing_A_review_of_recent_research

Oglesby-Neal, A., & Warnberg, C. (2019, February). *Law Enforcement Social Media Policies - Urban Institute*. Law Enforcement Social Media Policies Recommendations to Support Community Engagement . https://www.urban.org/sites/default/files/publication/99788/law_enforcement_social_media_policies_5.pdf

Oh, G., Zhang, Y., & Greenleaf, R. G. (2022). Measuring Geographic Sentiment toward Police Using Social Media Data. *American Journal of Criminal Justice*, *47*(5), 924–940. https://doi.org/10.1007/s12103-021-09614-z

Omand, D., Bartlett, J., & Miller, C. (2012). Introducing social media intelligence (SOCMINT). *Intelligence and National Security*, *27*(6), 801–823. https://doi.org/10.1080/02684527.2012.716965

Packingham v. North Carolina, 582 U.S. ___ (2017), Packingham v. North Carolina (U.S. Supreme Court June 19, 2017). Retrieved from https://supreme.justia.com/cases/federal/us/582/15-1194/.

Parkin, W. S., & Rice, S. K. (2016, December 5). *Social Media and Law Enforcement Investigations*. Oxford Academic. https://doi.org/10.1093/oxfordhb/9780199935383.013.98

Pasco Sheriff's Office. (n.d.). *Pasco Sheriff's Office Social Media Plan*. Pasco Sheriff's Office Social Media Plan. https://www.sheriffs.org/sites/default/files/Pasco%20Social%20Media%20Plan.pdf

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), 205630511773334. https://doi.org/10.1177/2056305117733344

Pearsall, B. (2010, June 22). *Predictive policing: The future of law enforcement?* National Institute of Justice. https://nij.ojp.gov/topics/articles/predictive-policing-future-law-enforcement

Pennsylvania State Police. (2016, November 15). *RTKL regulations and Operations Manuals*. Real-Time Open-Source-Based Investigations and Research AR 6-9. https://www.psp.pa.gov/contact/Pages/RTKL-REGULATIONS-AND-OPERATIONS-MANUALS.aspx?Paged=TRUE&p_SortBehavior=0&p_FileLeafRef=AR%2B7-12.pdf&p_ID=26&PageFirstRow=61&&View=%7BC9B28FFF-B4E7-4572-9ED3-F9A910D7A492%7D

Perry, W., McInnis, B., Price, C., Smith, S., & Hollywood, J. (2013). *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. https://doi.org/10.7249/rr233

Philadelphia Police Department. (2012, June 7). *Social Media and Networking*. Philadelphia Police Department Directive 6.10. https://www.phillypolice.com/assets/directives/D6.10-SocialMediaAndNetworking.pdf

Police1. (2010, December 29). *Sample Police Department Social Media Policies*. Social Media for Cops. https://www.police1.com/social-media-for-cops/articles/sample-police-department-social-media-policies-jKo6mikARPi0pC8T/

Proofpoint. (2023, September 18). *What is electronic communication? - Digital Comms explained: Proofpoint us*. Proofpoint. https://www.proofpoint.com/us/threat-reference/electronic-communication

Real-time event and risk detection. Dataminr. (2024, June 12). https://www.dataminr.com/

Rønn, K. V., Rasmussen, B. K., Roer, T. S., & Meng, C. (2021). On the Perception and Use of Information from Social Media in Investigative Police Work: Findings from a Scandinavian Study. *Policing: A Journal of Policy & Practice, 15*(2), 1262–1273. https://doi.org/10.1093/police/paaa028 San Francisco Police Department. (2023, October 17).

Social Media Policy. San Francisco Police Department. https://www.sanfranciscopolice.org/your-sfpd/policies/social-media-policy

SEASKATE, INC. (1998, July 1). The evolution and development of Police Technology. https://www.ojp.gov/pdffiles1/Digitization/173179NCJRS.pdf

Seattle Police Department. (2024, June 11). *Seattle Police Department Policy Manual*. PowerDMS. https://public.powerdms.com/Sea4550/tree/documents/2374801

Sepulvado, J. (2020, June 2). *Black lives matter report: Tweet quoting public enemy prompted DOJ investigation*. opb. https://www.opb.org/news/article/black-lives-matter-report-tweet-quoting-public-enemy-prompted-doj-investigation/

Shorr, J., McKay, J., & T. Primrose. (2023, November 3). *Forensic Technology Center of excellence*. Just Forensics In The Digital Age. https://forensiccoe.org/podcast-2023-case-studies-ep5/

Shah, S. (2016, May 14). *The history of Social Media*. Digital Trends. https://www.digitaltrends.com/computing/the-history-of-social-networking/

Singh, G. (2023, April 25). *LEMF (law enforcement monitoring facilities)*. Telecom Trainer. https://www.telecomtrainer.com/lemf-law-enforcement-monitoring-facilities/

Smith, A. (2024, May 30). *How to collect and mine your social media data for Growth*. Sprout Social. https://sproutsocial.com/insights/social-media-data-collection/

SocialNet - investigate social networks, profiles, links and activity. ShadowDragon.io. (2024, March 25). https://shadowdragon.io/socialnet/

Sozio, M. B. (2017, April 27). *Authenticating digital evidence at trial*. Authenticating Digital Evidence at Trial. https://www.americanbar.org/groups/business_law/resources/business-law-today/2017-april/authenticating-digital-evidence-at-trial/

Tirado, J. M. (2020, September 2). Bureau of Counterterrorism BCT Special Order 20-01 Utilization of Social Media. https://www.aclu-il.org/sites/default/files/cpd_bct_so_20-01_utilization_of_social_media_02_sep_20_version.pdf-compressed.pdf

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. https://doi.org/10.1177/1367549415577396

US Department of Justice Computer Crime and Intellectual Property Section (CCIPS). (2009, October). Facebook Account Search Warrant Affidavit. https://www.eff.org/files/filenode/facebook_draft_search_warrant_crim_sn.pdf

U.S. Department of Justice. (1999, November). *Online investigative principles for federal ...* Online investigative principles for federal law enforcement AGENTS. https://info.publicintelligence.net/DoJ-OnlineInvestigations.pdf

U.S. Department of Justice. (2022). *LAPD: 2022 Digital Evidence Management and Integration Project*. Bureau of Justice Assistance. https://bja.ojp.gov/funding/awards/15pbja-22-gg-03295-bwcx

United States Conference of Mayors. (2020, August 13). *Transparency and accountability to reinforce constitutional policing*. United States Conference of Mayors. https://www.usmayors.org/issues/police-reform/transparency-and-accountability-to-reinforce-constitutional-policing/

Villasenor, J., Nicol Turner Lee, J. V., & Wheeler, T. (2020, July 20). *How to reform police monitoring of social media*. Brookings. https://www.brookings.edu/articles/how-to-reform-police-monitoring-of-social-media/

Volle, A. (n.d.). *Creative commons*. Encyclopædia Britannica. https://www.britannica.com/topic/Creative-Commons

Waters, G. (2012, November 1). *Social Media and Law Enforcement*. FBI. https://leb.fbi.gov/articles/featured-articles/social-media-and-law-enforcement

Watson, D. M. (2023, July 28). DHS use of social media and other third-party digital ... https://www.dhs.gov/sites/default/files/2023-08/23_0803_mgmt_social-media-thrird-party-services-262-19-001.pdf

X. (n.d.). *Law enforcement*. Help Center. https://help.x.com/en/forms/law-enforcement

Xhafa, F., & Schneider, P. (2022). *Rapidminer*. Rapidminer - an overview | ScienceDirect Topics. https://www.sciencedirect.com/topics/computer-science/rapidminer

Appendix A

Austin, TX Police Department (Chacon, *Austin Police Department General Orders* 2021)

- **Contemplated uses for social media (other than public-facing use) and requirements for use in investigations:**
  - The policy provides that social media may be used only for a "valid law enforcement purpose," which includes "crime analysis and situational assessment reports; criminal intelligence development; or criminal investigations." The policy goes on to say that police department employees may only "seek or retain" information on social media when the information is "based on a criminal predicate or threat to public safety, is relevant to the investigation and prosecution of suspected criminal incidents, resulting justice system response, enforcement of sanctions, orders, or sentences, or the prevention of crime; or is useful in crime analysis or situational assessment reports for administration of criminal justice and public safety." The policy also permits the use of social media when there is "reasonable suspicion that an identifiable individual or organization" is engaged in criminal conduct or poses a threat to others and the information to be obtained from social media is "relevant to the criminal conduct or activity." The policy directs officers to evaluate social media for reliability and validity.
- **Prohibitions on the use of social media:**
  - The policy prohibits using social media to "seek or retain information" about individuals or organizations based on various protected categories. These include religion, political association, social views or activities, race, ethnicity, citizenship, place of origin, disability, gender, or sexual orientation (except for the categories from race through sexual orientation, where those characteristics are "relevant to individual's criminal conduct or activity" or are needed for identification). Social media also may not be used to collect or retain information about an "individual's participation in the particular non-criminal organization or lawful event," or about an individual's age, unless to determine if the person is a minor.
- **Specific rules for situational awareness or other non-investigative efforts:**
  - Crime analysis and situational assessment reports may be used for "special events management, including First Amendment-protected activities." Social media information must be deleted within 14 days if there is no related criminal activity.
- **Authorization required for general uses:**

        - No authorization is required for "general research, topical information, or other law enforcement uses" as long as those uses do not require an online alias.

    - **Limitations on undercover/covert activity:**
        - Use of an online alias requires a criminal predicate or threat to public safety or reasonable suspicion that an identifiable individual or organization has committed a crime or is involved in or is planning criminal conduct or activity that presents a threat to an individual, the community, or the nation, and the information is relevant to the criminal conduct or activity.

        - Employees must get approval from their supervisor to use an online alias based on evaluating whether an online alias would serve a valid law enforcement purpose. The policy establishes a specific approval process and requires deconfliction through the local fusion center (the Austin Regional Intelligence Center). All approved undercover activity requests must be reviewed at least every 90 days by a supervisor and will be discontinued if the activity does not provide information regarding a valid law enforcement purpose. Employees with an approved online alias can use it to "make false representations in concealment of personal identity in order to establish social media accounts."
        -

        - The policy specifies that "online undercover activity" entails interaction with an individual online, not simply surveillance. Employees may only undertake online undercover operations "when there is reason to believe that criminal offenses have been, will be, or are being committed (e.g., internet chat rooms where child exploitation occurs).

    - **Language governing use of personal device or account:**
        - The policy does not contain language regulating department employees' use of personal devices or accounts to access social media data.

- **Discussion of constitutional rights:**
    - The policy states that the Austin Police Department "will not seek or retain information about individuals or organizations solely based on their religion, political association, social views or activities [or an] individual's participation in a particular non-criminal organization or lawful event." The policy states that the department will not use social media to seek or retain information on an individual based on their protected characteristics unless they are "relevant to the individual's criminal conduct or activity or if required to identify the individual.

    - The policy allows officers to use social media monitoring tools to prepare crime analysis and situational awareness reports for special events,

including First Amendment-protected activities. However, if there was no criminal activity, information related to an event obtained through the social media monitoring tool will not be retained for more than 14 days.

Baltimore, MD Police Department **(Policy 604)** (Baltimore Police Department, *Social Media* 2016)

- **Contemplated uses for social media (other than public-facing use) and requirements for use in investigations:**
  - The policy states that "the Chief of the Criminal Investigation Division shall consult with the Director of the MRS when there is a belief that an ongoing investigation or intelligence collection effort would benefit from the use of social media. It may be appropriate for members to use non-official BPD social media accounts during a legitimate criminal investigation or during intelligence collection efforts related to public safety or potential criminal activity." It offers no additional guidance regarding investigative use (Page 4).
- **Prohibitions on the use of social media:**
  - "Only the Police Commissioner, his/her designee, the MRS Director, or a designated departmental spokesperson may post, comment or reply on a social media site on behalf of the Baltimore Police Department" (Page 4).
- **Specific rules for situational awareness or other non-investigative efforts:**
  - No rules for situational awareness or other non-investigative efforts.
- **Authorization required for general use:**
  - Authorization required for non-covert investigative uses (Page 4).
- **Limitations on undercover/covert activity:**
  - No specific language on undercover or covert social media accounts.
- **Language governing the use of personal devices or accounts:**
  - Investigative units may use non-official social media accounts for investigative purposes with the written permission of the Police Commissioner.
- **Designation of special use areas:**
  - There is no designation of special use areas.
- **Training of personnel:**
  - There is no training requirement mentioned.
- **Retention and storage of information and procedures for electronic evidence.**
  - This is not addressed in the policy.
- **Discussion of constitutional rights:**

- No language addressing the possible impact of the collection or viewing of social media upon individuals' or groups' constitutional rights.

Chicago, IL Police Department (Chicago Police Department, *Chicago Police Department general order G09-01-06 use of social media ...* 2023) (General Order G09-01-06)

- **Contemplated uses for social media (other than public-facing use) and requirements for use in investigations:**
  - In Section V, the policy for the use of social media outlets is delineated. states that "social media is a valuable tool when seeking evidence or information regarding missing persons, wanted persons, gang activity, crimes perpetuated online and/or photographs or videos of a crime to assist in case solvability." It does not offer any additional guidance regarding investigative use.

- **Prohibitions on the use of social media:**
  - Prohibitions on the use of social media include disparaging posts and department information (Sections I.(A)(2) and II(D).

- **Specific rules for situational awareness or other non-investigative efforts:**
  - No rules for situational awareness or other non-investigative efforts.

- **Authorization required for general use:**
  - "All Department social media outlets will be approved by the Superintendent or a designee."

- **Limitations on undercover/covert activity:**
  - No language on the use of undercover or covert social media accounts.

- **Language governing the use of personal devices or accounts:**
  - Investigative units will "use only Department-approved electronic equipment…" "…and conduct an investigation only while on duty…". (Section C 1. And 2.)

- **Designation of special use areas:**
  - There is no designation of special use areas.

- **Training of personnel:**
  - There is no training requirement mentioned.

- **Retention and storage of information and procedures for electronic evidence.**
  - This is not addressed in the policy.

- **Discussion of constitutional rights:**
  - Section C. 3. A. and b. address “The First Amendment” and “Investigations Directed at First Amendment-Related Information”. Both contain links to detailed information.

Not included in Chicago Police’s social media policy is an instruction from its Bureau of Counterterrorism directing training for investigations and intelligence gathering (Chicago Police Department, 2020). Bureau of Counterterrorism BCT Special Order 20-0 is a social media policy restricted to the department and not for release to the public. This policy is more detailed and inclusive.

Department **of Homeland Security (Directive 6.10 07-06-2012)** (Watson, *DHS use of social media and other third-party digital* ... 2023), (Callahan, Privacy Policy for Operational Use of Social Media 2012)

- **Contemplated uses for social media (other than public-facing use) and requirements for use in investigations:**
  - The policy contains the instruction regarding "monitor non-DHS accounts for nonoperational situation awareness related to DHS missions and activities." There is no specific language regarding gathering information for intelligence or investigation.
  - Operational use in investigations or obtaining official information (Page 3),
  - Situational awareness (Pages 1 & 4),
  - Intelligence and counterintelligence (Page 1).
- **Prohibitions on the use of social media:**
  - The policy contains prohibitions on the personal use of social media (Pages 13, 14, 15 & 16).
  - **Specific rules for situational awareness or other non-investigative efforts:** Defines situational awareness (Page 3).
- **Authorization required for general use:**
  - The DHS Assistant Secretary for Public Affairs approves social media (Page 5).
  - Requires approval of the component head (Page 7).
- **Limitations on undercover/covert activity:**
  - No language on undercover or covert social media accounts".
- **Language governing the use of personal devices or accounts:**
  - The policy addresses using personal devices or accounts (Page 13).
- **Designation of special use areas:**
  - There is no designation of special use areas.

- **Training of personnel:**
  - There is no training requirement mentioned.

- **Retention and storage of information and procedures for electronic evidence.**
  - Records management is addressed (pages 19 & 20).

  - The policy includes a section on documentation and retention (Page 9)
  -

- **Discussion of constitutional rights:**
- No language addressing the possible impact of the collection or viewing of social media upon individuals' or groups' constitutional rights. The policy has a list of statutory references dealing with legal topics (Pages 1, 2 & 3).

Detroit, MI Police Department (Department internet usage/web pages / social networking – 102.8 2020)

- **Contemplated uses for social media (other than public-facing use) and requirements for use in investigations:**
  - The policy provides written guidelines on Department and member uses of social media and the retention and release of information (page 1).
- **Prohibitions on the use of social media:**
  - Lists prohibited uses (Pages 4, 6, & 8).
- **Specific rules for situational awareness or other non-investigative efforts:**
  - Does not address situational awareness.
- **Authorization required for general use:**
  - Requires approval of the supervisor (Page 5).
- **Limitations on undercover/covert activity:**
  - The policy has specific instructions for using online activities (Pages 5 & 6).
- **Language governing the use of personal devices or accounts:**
  - Requires the Chief of Police's approval (Page 5).
- **Designation of special use areas:**
  - There is no designation of special use areas.
- **Training of personnel:**
  - There is no training requirement mentioned.
- **Retention and storage of information and procedures for electronic evidence.**
  - The policy includes a section on documentation and retention (Page 9).
- **Discussion of constitutional rights:**
  - Does not address First and Fourth Amendment concerns but does prohibit investigation of a person's "religion, race, ethnicity, citizenship, place of origin, disability, gender, or sexual orientation unless such information is relevant" (Page 7).

Los Angeles, CA Police Department (Los Angeles, CA Police Department, *Social Media User Guide* 2015)

- **Contemplated uses for social media (other than public-facing use) and requirements for use in investigations:**
  - The policy states that "it provides direction on Department-sanctioned uses of social media: as an integral part of the community relations mission, for situational awareness, and as an investigative tool (page 3).
- **Prohibitions on the use of social media:**
  - Lists prohibited uses (Page 7).
- **Specific rules for situational awareness or other non-investigative efforts:**
  - Defines situational awareness and lists examples (Page 5).
- **Authorization required for general use:**
  - Requires approval of the commanding officer (Page 6).
- **Limitations on undercover/covert activity:**
  - The policy has specific instructions for using online aliases (Pages 3 & 6).
- **Language governing the use of personal devices or accounts:**
  - Requires commanding officer's approval (Page 7).
- **Designation of special use areas:**
  - There is no designation of special use areas.
- **Training of personnel:**
  - There is no training requirement mentioned.
- **Retention and storage of information and procedures for electronic evidence.**
  - LAPD has a separate policy for handling electronic evidence (*LAPD: 2022 Digital Evidence Management and Integration Project* 2022).
- **Discussion of constitutional rights:**
  - Addresses both First and Fourth Amendment concerns (Page 4).

New York, NY Police Department (New York City Police Department, *Use of Social Networks for Investigative Purposes-General Procedure* 2012) (Operations Order Number: 34)

- **Contemplated uses for social media (other than public-facing use) and requirements for use in investigations:**
  - The policy states, "Data contained on the Internet within social network sites may assist law enforcement in gathering timely information in furtherance of crime prevention, including the preservation of public order and the investigation of criminal activity, including suspected terrorist activity. To effectively fulfill these duties, it may be necessary for service members to access social network sites using an online alias. (Page 1)

- **Prohibitions on the use of social media:**
  - No prohibitions on the use of social media. (Page 1).
- **Specific rules for situational awareness or other non-investigative efforts:**
  - No rules for situational awareness or other non-investigative efforts.

- **Authorization required for general use:**
  - Requires authorization from the deputy commissioner or the bureau chief (Page 2). No prior authorization is required for information contained on publicly available internet sources.

- **Limitations on undercover/covert activity:**
  - The policy has specific instructions for using online aliases (Pages 1, 2, & 5.

- **Language governing the use of personal devices or accounts:**
  - Limited to department-issued laptops with masked identification on a confidential internet connection (aircard), (Page 4).

- **Designation of special use areas:**
  - There is no designation of special use areas.
- **Training of personnel:**
  - There is no training requirement mentioned.

- **Retention and storage of information and procedures for electronic evidence.**
  - This is not addressed in the policy.

- **Discussion of constitutional rights:**
  - No language addressing the possible impact of the collection or viewing of social media upon individuals' or groups' constitutional rights. There are references to other material, such as the Federal Electronic Communications Privacy Act and obtaining a search warrant (Pages 3 & 4)

Philadelphia, PA Police Department **(Directive 6.10 07-06-2012)** (Philadelphia Police Department, *Social Media and Networking* 2012)

- **Contemplated uses for social media (other than public-facing use) and requirements for use in investigations:**
  - The policy contains no specific language for gathering intelligence or investigation information.

- **Prohibitions on the use of social media:**
  - The policy contains prohibitions on the personal use of social media (Pages 3, 5 & 6).

- **Specific rules for situational awareness or other non-investigative efforts:**
  - No rules for situational awareness or other non-investigative efforts.

- **Authorization required for general use:**
  - "Police department employees seeking to represent the department via social media outlets (e.g., individual or unit web page, Facebook, Twitter, MySpace, etc.) shall obtain express permission from the Police Commissioner or his/ her designee, before engaging in such activity" (Page 4).

- **Limitations on undercover/covert activity:**
  - No language on undercover or covert social media accounts".

- **Language governing the use of personal devices or accounts:**
  - "While in on-duty status, employees are prohibited from using privately-owned property to engage in personal use of social media" (Pages 3 & 5).

- **Designation of special use areas:**
  - There is no designation of special use areas.

- **Training of personnel:**
  - There is no training requirement mentioned.

- **Retention and storage of information and procedures for electronic evidence.**
  - This is not addressed in the policy.

- **Discussion of constitutional rights:**
- No language addressing the possible impact of the collection or viewing of social media upon individuals' or groups' constitutional rights. It contains a directive to "adhere to…existing federal, state, and local laws" (Pages 2 & 3).

U.S. Government Law Enforcement Agencies (Online Investigative Principles for Federal Law Enforcement Agents**)** (The Online Investigations Working Group, 1999)

- **Contemplated uses for social media (other than public-facing use) and requirements for use in investigations:**
  - The policy contains specific language regarding gathering information for intelligence or investigation.

- **Prohibitions on the use of social media:**
  - The policy contains prohibitions on accessing restricted sources (Page ix).

- **Specific rules for situational awareness or other non-investigative efforts:**
  - Rules for situational awareness or other non-investigative efforts are mentioned in "Emerging Resources", (Appendix A, Page 5).

- **Authorization required for general use:**
  - "Police department employees seeking to represent the department via social media outlets (e.g., individual or unit web page, Facebook, Twitter, MySpace, etc.) shall obtain express permission from the Police Commissioner or his/ her designee, before engaging in such activity" (Page 4).

- **Limitations on undercover/covert activity:**
  - Principle 6 covers "Online Communications" (Page ix), Principle 7 (Online Undercover Facilities" (Page x), "Online Undercover Operations", Pages 36-49), and Appropriating Online Identity", (Pages 54-58).

- **Language governing the use of personal devices or accounts:**
  - "While not in-on-duty status, employees may engage in online pursuits; if engaged in official business, the same rules apply as in on-duty status. (Page xi), and (Pages 59-61)..

- **Designation of special use areas:**
  - There is a designation of special use areas, "Online Undercover Facilities" (Pages 42-49).

- **Training of personnel:**
  - There is no training requirement mentioned.

- **Retention and storage of information and procedures for electronic evidence.**
  - This is addressed in “Preserving Records” (Pages 31-33).the policy.

- **Discussion of constitutional rights:**
  - Language addressing the “Privacy Act,” “Electronic Communications Act,” and the First and Fourth Amendments of the Constitution on numerous pages, including “Accessing Restricted Sources” (Pages 25-29).