

DEVELOPING A POLICY ON THE  
**USE OF SOCIAL MEDIA**  
IN INTELLIGENCE AND INVESTIGATIVE ACTIVITIES

GUIDANCE AND RECOMMENDATIONS

FEBRUARY 2013





DEVELOPING A POLICY ON THE  
**USE OF SOCIAL MEDIA**  
IN INTELLIGENCE AND INVESTIGATIVE ACTIVITIES

---

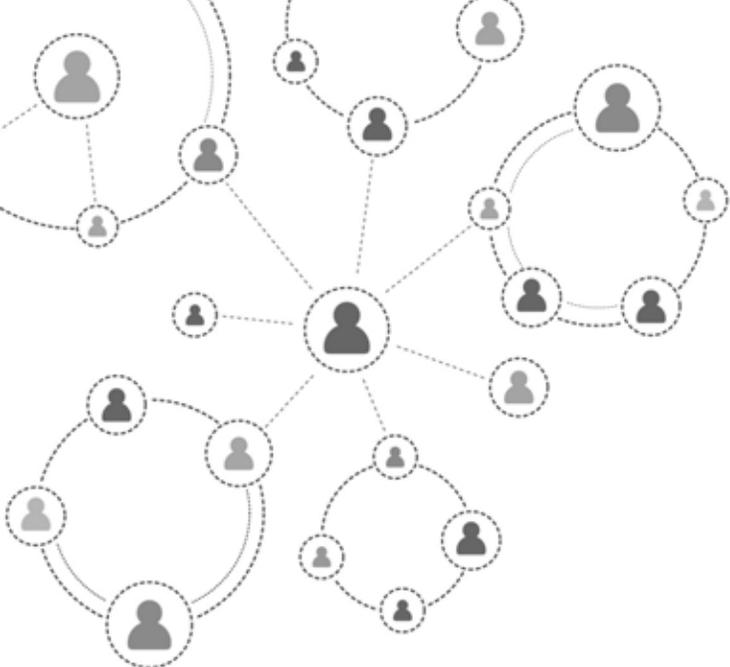
GUIDANCE AND RECOMMENDATIONS

# TABLE OF CONTENTS

---

Executive Summary.....	1
Introduction .....	5
Social Media Policy Elements.....	11
Conclusion .....	19
Appendix A—Cases and Authorities.....	21
Appendix B—Georgia Bureau of Investigation Social Media Policy.....	29
Appendix C—Dunwoody Police Department Social Media Policy.....	37
Appendix D—New York City Police Department Social Media Policy .....	41

This project was supported by Grant No. 2010-MU-BX-K019 awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, in collaboration with the Global Justice Information Sharing Initiative. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Justice.



## EXECUTIVE SUMMARY

The advent of social media sites has created an environment of greater connection among people, businesses, and organizations, serving as a useful tool to keep in touch and interact with one another. These sites enable increased information sharing at a more rapid pace, building and enhancing relationships and helping friends, coworkers, and families to stay connected. Persons or groups can instantaneously share photos or videos, coordinate events, and/or provide updates that are of interest to their friends, family, or customer base. Social media sites can also serve as a platform to enable persons and groups to express their First Amendment rights, including their political ideals, religious beliefs, or views on government and government agencies. Many government entities, including law enforcement agencies, are also using social media sites as a tool to interact with the public, such as posting information on crime trends, updating citizens on community events, or providing tips on keeping citizens safe.

---

*Social media sites are increasingly being used to instigate or conduct criminal activity, and law enforcement personnel should understand the concept and function of these sites, as well as know how social media tools and resources can be used to prevent, mitigate, respond to, and investigate criminal activity.*

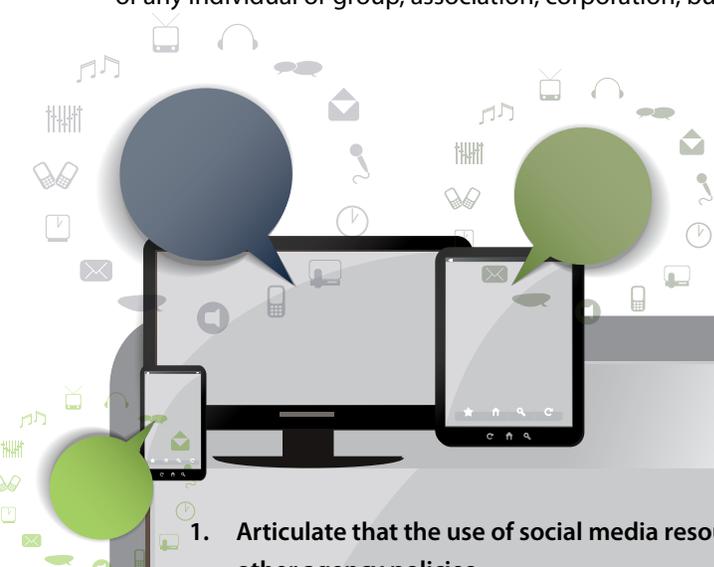
---

Social media sites have become useful tools for the public and law enforcement entities, but criminals are also using these sites for wrongful purposes. Social media sites may be used to coordinate a criminal-related flash mob or plan a robbery, or terrorist groups may use social media sites to recruit new members and espouse their criminal intentions. Social media sites are increasingly being used to instigate or conduct criminal activity, and law enforcement personnel should understand the concept and function of these sites, as well as know how social media tools and resources can be used to prevent, mitigate, respond to, and investigate criminal activity. To ensure that information obtained from social media sites for investigative and criminal intelligence-related activity is used lawfully while also ensuring that individuals' and groups' privacy, civil rights, and civil liberties are protected, law enforcement agencies should have a social media policy (or include the use of social media sites in other information-related policies). This social media policy should communicate how information from social media sites can be utilized by law enforcement, as well as the differing levels of engagement—such as apparent/overt, discrete, or covert—with subjects when law enforcement personnel access social media sites, in addition

to specifying the authorization requirements, if any, associated with each level of engagement. These levels of engagement may range from law enforcement personnel “viewing” information that is publicly available on social media sites to the creation of an undercover profile to directly interact with an identified criminal subject online. Articulating the agency’s levels of engagement and authorization requirements is critical to agency personnel’s understanding of how information from social media sites can be used by law enforcement and is a key aspect of a social media policy.

Social media sites and resources should be viewed as another tool in the law enforcement investigative toolbox and should be used in a manner that adheres to the same principles that govern all law enforcement activity, such as actions must be lawful and personnel must have a defined objective and a valid law enforcement purpose for gathering, maintaining, or sharing personally identifiable information (PII). In addition, any law enforcement action involving undercover activity (including developing an undercover profile on a social media site) should address supervisory approval, required documentation of activity, periodic reviews of activity, and the audit of undercover processes and behavior. Law enforcement agencies should also not collect or maintain the political, religious, or social views, associations, or activities of any individual or group, association, corporation, business, partnership, or organization unless there is a legitimate

public safety purpose. These aforementioned principles help define and place limitations on law enforcement actions and ensure that individuals’ and groups’ privacy, civil rights, and civil liberties are diligently protected. When law enforcement personnel adhere to these principles, they are ensuring that their actions are performed with the highest respect for the



## A SOCIAL MEDIA POLICY SHOULD ADDRESS THESE KEY ELEMENTS

1. Articulate that the use of social media resources will be consistent with applicable laws, regulations, and other agency policies.
2. Define if and when the use of social media sites or tools is authorized (as well as use of information on these sites pursuant to the agency’s legal authorities and mission requirements).
3. Articulate and define the authorization levels needed to use information from social media sites.
4. Specify that information obtained from social media resources will undergo evaluation to determine confidence levels (source reliability and content validity).
5. Specify the documentation, storage, and retention requirements related to information obtained from social media resources.
6. Identify the reasons and purpose, if any, for off-duty personnel to use social media information in connection with their law enforcement responsibilities, as well as how and when personal equipment may be utilized for an authorized law enforcement purpose.
7. Identify dissemination procedures for criminal intelligence and investigative products that contain information obtained from social media sites, including appropriate limitations on the dissemination of personally identifiable information.

law and the community they serve, consequently fostering the community's trust in and support for law enforcement action.

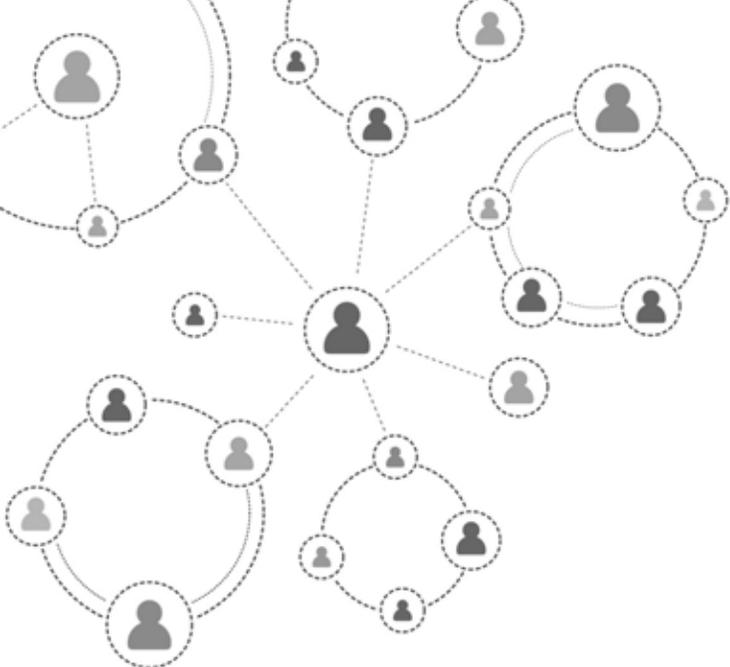
The Bureau of Justice Assistance (BJA)—with the support of the Global Justice Information Sharing Initiative (Global) Advisory Committee (GAC), a Federal Advisory Committee (FAC) to the U.S. Attorney General on justice-related information sharing, and the Criminal Intelligence Coordinating Council (CICC)—has developed the resource *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations*, which provides law enforcement leadership and policymakers with recommendations and issues to consider when developing policy related to the use of social media information for criminal intelligence and investigative activities. A social media-related policy (or a policy that includes procedures on the use of social media information) will help protect the law enforcement agency and agency personnel and will also help ensure the continued protection of privacy, civil rights, and civil liberties of individuals and groups in the community.

The *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations* is designed to guide law enforcement agency personnel through the development of a social media policy by identifying elements that should be considered when drafting a policy, as well as issues to consider when developing a policy, focusing on privacy, civil rights, and civil liberties protections. This resource can also be used to modify and enhance existing policies to include social media information. All law enforcement agencies, regardless of size and jurisdiction, can benefit from the guidance identified in this resource.

The key elements identified in this resource can be applied to “traditional” social media sites (such as Facebook, Twitter, and YouTube) and are also applicable as different and new types of social media sites emerge and proliferate. As a policy is developed, the agency privacy officer and/or legal counsel should be consulted and involved in the process. Additionally, many agencies have an existing privacy policy that includes details on how to safeguard privacy, civil rights, and civil liberties, and an agency's social media-related policy should also communicate how these protections will be upheld when using information obtained from social media sites.

Social media sites have emerged as a method for instantaneous connection among people and groups; information obtained from these sites can also be a valuable resource for law enforcement in the prevention, identification, investigation, and prosecution of crimes. To that end, law enforcement leadership should ensure that their agency has a social media policy that outlines the associated procedures regarding the use of social media-related information in investigative and criminal intelligence activities, while articulating the importance of privacy, civil rights, and civil liberties protections. Moreover, the same procedures and prohibitions placed on law enforcement officers when patrolling the community or conducting an investigation should be in place when agency personnel are accessing, viewing, collecting, using, storing, retaining, and disseminating information obtained from social media sites. As these sites increase in popularity and usefulness, a social media policy is vital to ensuring that information from social media used in criminal intelligence and investigative activities is lawfully used, while also ensuring that individuals' and groups' privacy, civil rights, and civil liberties are diligently protected.





## INTRODUCTION

In recent years, social media sites<sup>1</sup> have emerged as a useful tool for friends, coworkers, and families to keep in touch and interact with one another. Persons and groups can share photos or videos, coordinate meet-ups or plans for the weekend, and/or provide updates on newsworthy events to their friends, family, or customer base. One of the goals of these types of sites is instantaneous connections among people, businesses, and organizations, leading to greater and quicker sharing of information and enhanced relationships. Social media sites can also serve as a platform to enable people to express their First Amendment rights, including their political ideals, religious beliefs, or disappointments with government agencies. Many government entities, including law enforcement agencies, are now using social media sites to interact with the public and provide information on crime trends and community events and tips for keeping citizens safe.

In addition to these types of information sharing exchanges between and among persons and entities, social media sites have become a tool that criminals are using for nefarious and criminal purposes. Examples of the use of social media to conduct criminal activity include individuals coordinating a criminal-related flash mob<sup>2</sup> or utilizing a social media site to plan a robbery, online predators joining a social media site to identify and interact with potential victims, and terrorist groups using social media to recruit new members and espouse criminal intentions. Because social media sites are increasingly being used to instigate and conduct criminal activity, law enforcement personnel should understand the concept and function of social media sites and know how social media tools and resources can be used to prevent, mitigate, respond to, and investigate criminal activity.

---

*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.*

---

<sup>1</sup> The International Association of Chiefs of Police's (IACP) Center for Social Media defines *social media* as "a category of Internet-based resources that integrate user-generated content and user participation. This includes, but is not limited to, social networking sites (Facebook, MySpace), microblogging sites (Twitter), photo- and video-sharing sites (Flickr, YouTube), wikis (Wikipedia), blogs, and news sites (Digg, Reddit)."

<sup>2</sup> A *flash mob* is a "group of people, usually organized through social media or text message, that gather at a location to perform a specific action before dispersing. These actions may be for entertainment or criminal purposes." (<http://www.IACPsocialmedia.org/glossary>)



Social media sites can be valuable sources of information for law enforcement personnel as they fulfill their public safety mission—agency public information officers may use social media to interact with the public, detectives may access social media sites to assist in the identification and apprehension of criminal subjects, intelligence analysts may utilize social media resources as they develop intelligence products regarding emerging criminal activity, and fusion center analysts may use social media resources to assist in the development of analytic assessments. 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.<sup>3</sup>

To assist agencies in drafting a social media policy, the Bureau of Justice Assistance (BJA)—with the support of the Global Justice Information Sharing Initiative (Global) Advisory Committee (GAC), a Federal Advisory Committee (FAC) to the U.S. Attorney General on justice-related information sharing, and the Criminal Intelligence Coordinating Council (CICC)—has developed this resource to provide law enforcement leadership and policymakers with recommendations and issues to consider related to the use of information obtained from social media sites as a part of criminal intelligence and investigative activities.<sup>4</sup>

It is recommended that all law enforcement leadership support the development of a social media-related policy and associated procedures (or enhance existing policies) to guide personnel on accessing, viewing, collecting, storing, retaining, and disseminating (or using) information from social media sites, tools, and resources as a part of their authorized investigative and criminal intelligence activities.<sup>5</sup> A written policy assists in the protection of the agency and agency personnel, as well as the individuals and groups in the community. With the advent of the Internet and, specifically, social media sites, the expectation of privacy has changed. Individuals and groups regularly make openly available various pieces of information of themselves (e.g., photos, relationship links, current locations, dates of birth); while in many cases this information is public and available to anyone with Internet access, law enforcement personnel should use this type of information only based upon a valid law enforcement purpose (i.e., consistent with legal authorities and mission requirements). A policy will assist agency personnel in identifying and understanding their purpose and limitations regarding the use of information from social media sites, the need to document this purpose, and the importance of protecting the public from inadvertent or intentional misuse of information obtained from social media sites.

This resource is designed to identify elements that should be considered for inclusion in a social media policy, issues to consider when developing a policy, and examples of the use of social media as an investigative or intelligence-related tool, focusing on the protection of privacy, civil rights, and civil liberties of individuals and groups. The tenets identified in this resource can be used to draft a new policy or enhance existing information and criminal intelligence-related policies.

<sup>3</sup> Agency leadership may also incorporate the tenets identified in the paper into existing policies and procedures (such as policies on criminal intelligence and/or criminal investigations).

<sup>4</sup> For purposes of this resource, *law enforcement* may be broadly defined to include all activities related to crime prevention or reduction and the enforcement of the criminal law. However, it is important to note that certain law enforcement or criminal justice agencies may be subject to additional constraints regarding access, use, or disclosure of social media sites and information. For example, prosecutors’ offices must adhere to constitutional and statutory discovery and ethical standards that would not apply to police agencies. Consequently, nonpolice law enforcement agencies (such as state attorneys’ offices or other prosecutorial entities) will need to take any unique considerations into account in developing a social media policy.

<sup>5</sup> For the purpose of this document, accessing, viewing, collecting, storing, retaining, and disseminating information obtained from social media sites, tools, and resources will be referred to as using information obtained from social media sites, tools, and resources.

## AUDIENCE



All law enforcement agencies, regardless of size—from a small, rural agency to a large, metropolitan law enforcement agency to a state or urban area fusion center—can benefit from the recommendations identified in this document. As agency policymakers review the components of this resource, it should be understood that social media is, in essence, simply another resource for law enforcement personnel to use in the performance of their public safety mission. The same basic policing principles apply in the use of social media as with other law enforcement action.<sup>6</sup> It is important to provide all agency personnel—from leadership to analysts to detectives and investigators to uniformed patrol officers—with pertinent and applicable guidance to

ensure that social media resources are being utilized in a lawful and appropriate manner, a manner that upholds the agency's mission and legal authorities and complies with applicable federal, state, and tribal laws and local ordinances. As agencies develop and adapt a policy on using social media information as a part of their investigative and intelligence-related activities (or enhance existing policies), it is recommended that the agency privacy officer and/or legal counsel be consulted and be involved in the development and implementation process.

## THE PROTECTION OF PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES



As with all law enforcement activity and actions, individuals' privacy, civil rights, and civil liberties must be diligently protected, and the proliferation of social media sites and technology has led to a renewed focus on these protections. Social media resources not only provide a new forum and format for free speech but also introduce a potential risk to individuals' privacy, civil rights, and civil liberties if unauthorized or inappropriate access or use occurs. To mitigate such risks, law enforcement officers and agency personnel are trained to ensure the protection of these rights while performing their duties, be it providing security at a public rally, conducting a criminal investigation, or developing

criminal intelligence.<sup>7</sup> This type of training may also be applicable to the use of social media sites in investigative and intelligence activities and the privacy, civil rights, and civil liberties implications associated with access to social media sites and the use of information obtained from such sites.

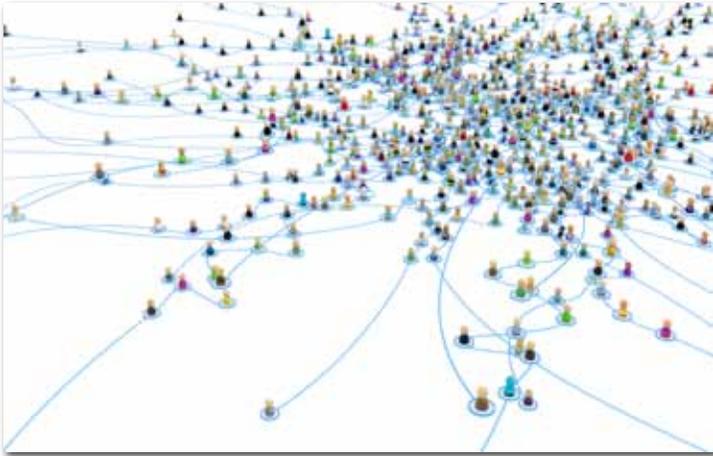
In addition to training, many agencies have a privacy policy that includes details on how to protect individuals' and groups' privacy, civil rights, and civil liberties.<sup>8</sup> To support and enhance the agency's privacy policy, agencies should also have a policy regarding social media (or enhance existing information and criminal intelligence-related policies) that articulates how these protections will be upheld when using information obtained from social media sites and resources.

6 See the section titled "Law Enforcement Principles" for additional information on these principles.

7 An example of privacy training for line officers is available at [http://www.ncirc.gov/training\\_privacylineofficer.cfm](http://www.ncirc.gov/training_privacylineofficer.cfm).

8 Additional information on how to develop a privacy policy is available at <http://www.it.ojp.gov/privacy>.

## USES OF SOCIAL MEDIA



Social media may be used by law enforcement personnel in their daily functions in a number of areas, including:

- Pre-employment background investigations
- Outreach and community engagement
- Emergency alerts and notifications
- Analytic assessments
- Situational awareness reports
- Intelligence development
- Criminal investigations

Additional guidance for law enforcement agencies and personnel regarding pre-employment background investigations, outreach and community engagement, and emergency alerts and notifications is accessible via the International Association of Chiefs of Police's (IACP) Center for Social Media Web site, <http://www.IACPsocialmedia.org/>.

Analytic assessments and situational awareness reports can be designed to provide information to law enforcement on a specific topic to assist agencies in maintaining public safety. These assessments may serve as a gauge for determining the types of criminal activity within a region or determining whether there are threats related to an upcoming public event.<sup>9</sup> Information from social media sites may be referenced in an analytic assessment that identifies current levels of criminal activity within an agency's jurisdiction. For example, an agency may search Twitter feeds, which may contain information on gang-related activities, and Flickr, which may include pictures of gang-related graffiti. This information may then be referenced in an assessment to provide examples of the types of gang activity occurring within a certain area.

As it relates to criminal intelligence development and criminal investigations, information from social media sites may be used as a part of criminal-related background investigative activities. For example, a criminal subject's Facebook page may be accessed to further support the identification of the subject and/or acquaintances. Social media sites and resources may also be used to determine a timeline of events for a suspect. For example, when a person "checks in" on the Web site FourSquare at a certain date and time, this information may be accessible by Facebook users. The individual may then post a picture of himself at this location, which may also be geotagged<sup>10</sup> via a smartphone and uploaded by the individual to Twitter.

There are an ever-increasing number and variety of social media sites: simple Web sites to post short pieces of information, virtual worlds (e.g., Club Penguin, Second Life, massively multiplayer online role-playing games, or online gambling sites), photo-sharing sites, and online forums and comment areas. Although this document will focus on "traditional" social media sites while acknowledging the continuing emergence and proliferation of different types of social media, it should be understood that the elements set forth in this paper may be applied to all types of social media sites and resources.

<sup>9</sup> Additional information on responding to First Amendment-protected events is found in the *Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies*, available at [http://it.ojp.gov/documents/First\\_Amendment\\_Guidance.pdf](http://it.ojp.gov/documents/First_Amendment_Guidance.pdf).

<sup>10</sup> The terms *geolocation/geotagging*, defined at [www.IACPsocialmedia.org/glossary](http://www.IACPsocialmedia.org/glossary), refer to the incorporation of location data in various media, such as, for instance, a photograph, a video, or an SMS message. This may be used on social media platforms to notify people where a user is at a given time.

## ELEMENTS OF A SOCIAL MEDIA POLICY



The purpose of a social media policy is to define and articulate acceptable law enforcement practices related to using information obtained from social media sites. As a part of a social media policy, agency leadership should reference other related policies and/or general orders regarding both criminal intelligence and criminal investigations, including an agency's privacy policy or policy regarding undercover activities. Because social media sites can be used to support these functions, it is important to ensure consistency and continuity between policies or orders.

Key elements of a social media policy include:

1. Articulate that the use of social media resources will be consistent with applicable laws, regulations, and other agency policies.
2. Define if and when the use of social media sites or tools is authorized (as well as use of information on these sites pursuant to the agency's legal authorities and mission requirements).
3. Articulate and define the authorization levels needed to use information from social media sites.
4. Specify that information obtained from social media resources will undergo evaluation to determine confidence levels (source reliability and content validity).
5. Specify the documentation, storage, and retention requirements related to information obtained from social media resources.
6. Identify the reasons and purpose, if any, for off-duty personnel to use social media information in connection with their law enforcement responsibilities, as well as how and when personal equipment may be utilized for an authorized law enforcement purpose.
7. Identify dissemination procedures for criminal intelligence and investigative products that contain information obtained from social media sites, including appropriate limitations on the dissemination of personally identifiable information (PII).

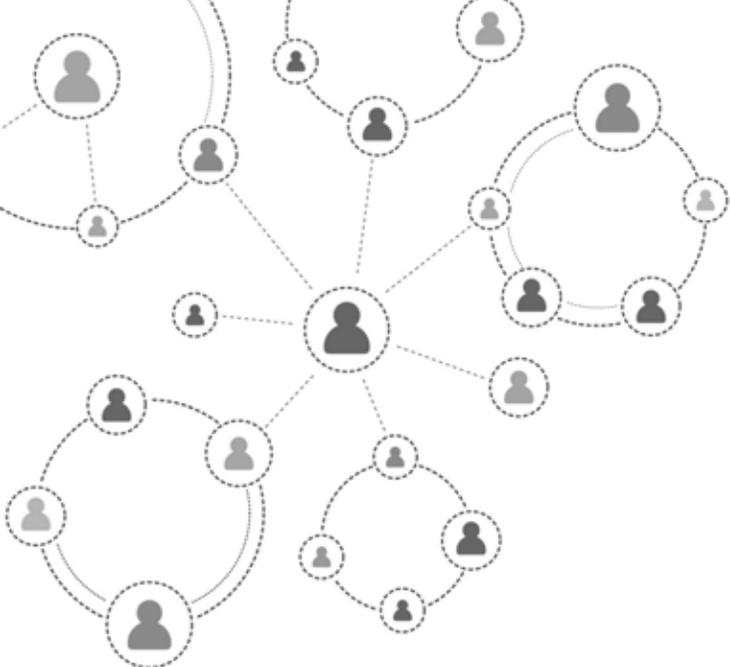
## LAW ENFORCEMENT PRINCIPLES



Interwoven within these policy elements is the acknowledgement that social media sites and resources are another tool in law enforcement's toolbox of information sources. As such, social media sites and resources should be utilized in a manner that adheres to the same principles that govern all law enforcement actions. These principles include:

- Law enforcement actions must be lawful.
  - Law enforcement actions should confirm with community standards, when appropriate.
  - Law enforcement actions must have a defined objective and a valid law enforcement purpose for gathering, maintaining, or sharing personally identifiable information about criminal subjects.
- Law enforcement agencies should not collect or maintain information about the political, religious, or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless there is a legitimate public safety purpose, such as the information directly relates to criminal conduct or activity. In the case of criminal intelligence, such information should not be collected or maintained unless there is reasonable suspicion to believe that the subject of the information is or may be involved in criminal conduct or activity and the information is directly related to the criminal conduct or activity.
  - Law enforcement policy directives must define:
    - » The circumstances under which conduct by personnel is authorized.
    - » The limitations on conduct by personnel.
  - All law enforcement officers and support personnel must be properly trained.
  - If law enforcement action involves undercover activity, the following areas should be addressed:
    - » Supervisory approval.
    - » Required documentation of activity.
    - » Periodic reviews of activity.
    - » Audit of undercover processes and behavior, including authorization time frames for undercover activities.

Regardless of the tools law enforcement personnel use to perform their duties, these principles help define and place limitations on actions undertaken by personnel and ensure the protection of individuals' and groups' privacy, civil rights, and civil liberties. The implementation of these principles will help ensure that all law enforcement action is performed with the highest respect for the law and for the community and will also help enhance the community's trust in law enforcement.



# SOCIAL MEDIA POLICY ELEMENTS

## ELEMENT 1

**ARTICULATE THAT THE USE OF SOCIAL MEDIA RESOURCES WILL BE CONSISTENT WITH APPLICABLE LAWS, REGULATIONS, AND OTHER AGENCY POLICIES.**

**Background:** Social media should be viewed as another tool in the law enforcement toolbox and should be subject to the same policies and guiding principles as other investigative methods and tools, including the identification of reasonable suspicion, a criminal predicate, or a criminal nexus and adherence to the agency's legal authorities and mission requirements.

**Action:** As a part of the agency's authorized law enforcement purpose, social media sites may be accessed to follow up on tips and leads, suspicious activity reports, investigative support, development of criminal intelligence, and the development of situational awareness reports. An agency policy on the use of social media resources as a part of investigative and intelligence-related activities should be similar to agency policies regarding the use of other investigative tools, such as undercover activities or accessing other types of open source information (e.g., Accurant or Internet-based search engines). Further, the social media policy should specify that personnel should be able to articulate the purpose of using information from social media sites, answering the questions "What are you using?" "Why are you using it?" "How did you use it?" and "Is there a time frame on its relevance?"

As a part of this continuity, a social media policy should specifically address:

- When the use of social media sites is authorized.
- The supervisory authorization process (if needed).
- Limitations on using information from social media sites.
- When and how social media sites may be accessed (e.g., during working hours or via agency resources).

## ELEMENT 2

### DEFINE IF AND WHEN THE USE OF SOCIAL MEDIA SITES OR TOOLS IS AUTHORIZED (AS WELL AS USE OF INFORMATION ON THESE SITES PURSUANT TO THE AGENCY'S LEGAL AUTHORITIES AND MISSION REQUIREMENTS).

**Background:** Agency leadership and policymakers should be knowledgeable of applicable laws and regulations (including the U.S. Constitution; the Bill of Rights, specifically the Fourth Amendment; the state constitution; other laws; and 28 CFR Part 23) when developing a social media policy and should know how these laws affect using information obtained from social media sites.

Law enforcement has an obligation to comply with the Fourth Amendment. Every person has the right to be free from “unreasonable searches and seizures” of their “persons, houses, papers, and effects.” These same protections may also apply towards the use of social media sites—the uploading of pictures, the posting of activities, and the relationships between and among individuals and groups. With the increasing use of technology and the free flow of information on the Internet, it may be difficult to discern what access is reasonable and what would be deemed unreasonable under the Fourth Amendment; therefore, a social media policy should clearly identify reasonable access to social media sites and the use of information obtained from social media sites.

In addition to the Fourth Amendment, the *Katz* test<sup>11</sup> establishes a method that can also be utilized as agency personnel analyze public or private information on social media sites. This test, based on *Katz v. United States*, 389 U.S. 347 (1967), which addresses the expectation of privacy and intent to make information private, could also be applied to the use of social media information, specifically whether a social media site user has exhibited an expectation of privacy in the information and whether the expectation is one that society is ready to recognize as reasonable. For information posted on the Internet (via a social media site) that a user has made no effort to make private or conceal, applying the principles of the *Katz* test would most likely result in a determination that the information is public. However, law enforcement personnel should use that information only when there is an identified, valid law enforcement purpose.

28 CFR Part 23 may also assist agencies as they develop a social media policy. The 28 CFR Part 23 federal regulation has become the de facto national standard regarding criminal intelligence information systems. Although 28 CFR Part 23 regulates systems, many of its tenets may be applicable to a policy regarding social media, such as storage, retention, and sharing of information obtained from social media sites and resources. Additionally, 28 CFR Part 23 states that a project “shall not collect or maintain criminal intelligence information about the political, religious, or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity.” This overarching purpose statement is also arguably pertinent to information obtained by law enforcement personnel via social media sites, specifically regarding what information personnel can store, retain, and disseminate on political, religious, or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization.

**Action:** A social media policy should articulate the parameters regarding using information obtained from social media sites. These parameters should be consistent with applicable laws, regulations, and other agency policies and further articulate how privacy, civil rights, and civil liberties protections are upheld during such activities. It is important to note that although information on many social media sites may be “open” (e.g., anyone with Internet access can view the information), **law enforcement must be mindful of what is legal, as well as what is consistent with community standards and expectations, when using information from a social media site.** In other words, simply because information is

11 See Appendix A for additional information on the *Katz* test and decision.

available to law enforcement does not mean it should be used by law enforcement in the absence of a clearly defined and valid law enforcement purpose. For example, a law enforcement investigator should search for and access an individual's Facebook profile when an authorized law enforcement purpose is identified, such as a search for a missing person or further identification of an alleged criminal, and not to look for information on a new neighbor.

Relevant investigative laws, regulations, and policies should also be referenced in a social media policy. Articulating laws, regulations, and policies, as they relate to the use of social media sites and information, will support the agency and personnel in ensuring that they are using social media for a valid law enforcement purpose, adhering to established law enforcement principles, and protecting citizens' and groups' privacy, civil rights, and civil liberties.

Additionally, a social media policy (or policy that addresses information obtained from social media sites) should address the ever-changing nature of social media and associated technology. Technology advancements may affect the access and collection of information from social media sites, and a policy should acknowledge that though technology may change, the foundational elements for accessing social media sites remain consistent, such as accessing social media sites for an authorized law enforcement purpose.

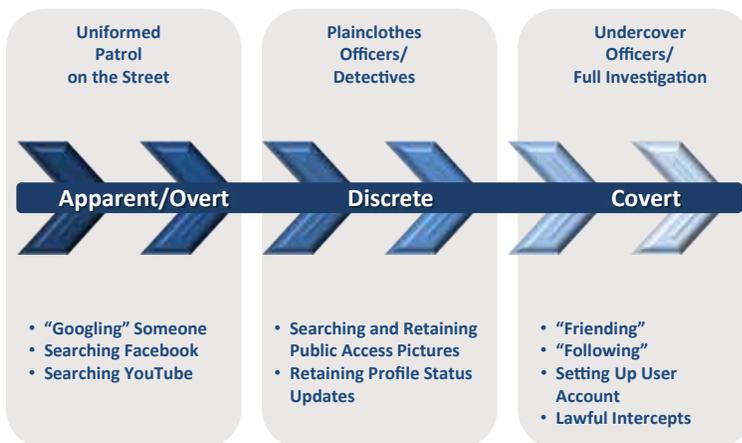
## ELEMENT 3 ARTICULATE AND DEFINE THE AUTHORIZATION LEVELS NEEDED TO USE INFORMATION FROM SOCIAL MEDIA SITES.

**Background:** Social media sites have varying and differing levels of access and engagement, ranging from “following” someone on Twitter to “friending” someone on Facebook or simply searching for an individual or a topic via Google. Engagement levels may also vary, from reviewing publicly available information on a social-networking site to accessing social media resources from a nongovernmental Internet Protocol (IP) address to creating a user profile or account for undercover operations to lawful intercepts of electronic information. Within the different engagement levels are privacy, civil rights, and civil liberties implications. A social media policy should articulate the levels of engagement by law enforcement personnel with subjects when accessing social media sites and also specify the authorization requirements associated with each level.

### Traditional Law Enforcement Actions



### Social Media Actions



As part of the levels of engagement, law enforcement personnel should understand privacy settings, end-user licensing agreements, and terms-of-service requirements. Users may regulate their privacy settings on their “profile,” which in turn could affect the level-of-engagement parameters. Additionally, companies may articulate law enforcement engagement parameters via a terms-of-service agreement.<sup>12</sup>

<sup>12</sup> Many Internet- and communication-based companies have developed guides to assist law enforcement in understanding what information is available and how that information may be obtained. Additional information on these guides is available at the IACP’s Center for Social Media, at <http://www.IACPsocialmedia.org/investigativeguides>.

To assist in understanding how information from social media sites can be used by law enforcement, the graphic above provides a visual demonstration of the comparison between traditional law enforcement practices and specific social media actions. As identified in the graphic, examples of levels of engagement include:

**Apparent/Overt Use**—In the Apparent/Overt Use engagement level, law enforcement’s identification need not be concealed. Within this engagement level, there is no interaction between law enforcement personnel and the subject/group. This level of access is similar to an officer on patrol. Information accessed via this level is open to the public (anyone with Internet access can “see” the information). Law enforcement’s use and response should be similar to how it uses and responds to information gathered during routine patrol. An example of Apparent/Overt Use would be agency personnel searching Twitter for any indication of a criminal-related flash mob to develop a situational awareness report for the jurisdiction.

Apparent/Overt Use is based on user profiles/user pages being “open”—in other words, anyone with Internet capabilities can access and view the user’s information. For instance, if an officer searches for a criminal subject’s Facebook page and determines that a profile which appears to be that of the subject has the account privacy settings set to “public” (meaning the information can be viewed by everyone), then the use of that information would be considered Apparent/Overt Use.

The authorization level for Apparent/Overt Use may be minimal, as this level of engagement is considered part of normal, authorized law enforcement activity (based on the law enforcement purpose).

**Discrete Use**—During the Discrete Use engagement level, law enforcement’s identity is not overtly apparent. There is no direct interaction with subjects or groups; rather, activity at this level is focused on information and criminal intelligence gathering. The activities undertaken during the Discrete Use phase can be compared to the activities and purpose of an unmarked patrol car or a plainclothes police officer. An example of Discrete Use is an analyst utilizing a nongovernmental IP address to read a Weblog (or blog)<sup>13</sup> written by a known violent extremist who regularly makes threats against the government. Bloggers (those who write or oversee the writing of blogs) may use an analytical tool to track both “hits” to the blog and IP addresses of computers that access the blog, which could potentially identify law enforcement personnel to the blogger. This identification could negatively impact the use of the information and the safety of law enforcement personnel, who would not want to reveal that they are accessing the blog for authorized law enforcement purposes. In many cases, direct supervisory approval may not be necessary within this level of engagement, but the policy should address agency protocol.

**Covert Use**—During the Covert Use engagement level, law enforcement’s identity is explicitly concealed. Law enforcement is engaging in authorized undercover activities for an articulated investigative purpose, and the concealment of the officer’s identity is essential. An example of Covert Use is the creation of an undercover profile to directly interact with an identified criminal subject online. Another example is an agency lawfully intercepting information from a social media site, through a court order, as a part of authorized law enforcement action. Clear procedures should be identified and documented on the use of social media in this phase, since there are many privacy, civil rights, and civil liberties implications associated with Covert Use. Agencies should also review social media sites’ information for law enforcement authorities and terms of service for additional information on undercover profiles.

Authorization levels for Covert Use activities should be clearly identified and could be compared to authorization levels needed for any undercover investigative activity (such as undercover narcotics investigations).

**Action:** An agency’s social media policy should identify the agency’s defined levels of engagement that will be utilized by agency personnel, the types of activity associated with these levels, and direct authorization requirements, if any,

<sup>13</sup> For additional information on blogs, please visit <http://www.IACPsocialmedia.org/blogfactsheet>.

associated with each level from use as a part of official law enforcement activities (e.g., the checking of social media sites is built into the analytic product development process) or direct supervisor approval requirements (such as development of an undercover profile to interact with a criminal subject). For example, if an agency uses social media to gather or disseminate information regarding a First Amendment-related event that has become violent in other jurisdictions, it is essential to clearly define any limits on the collection and use of information from social media.<sup>14</sup>

## ELEMENT 4

### SPECIFY THAT INFORMATION OBTAINED FROM SOCIAL MEDIA RESOURCES WILL UNDERGO EVALUATION TO DETERMINE CONFIDENCE LEVELS (SOURCE RELIABILITY AND CONTENT VALIDITY).

**Background:** The evaluation of information—be it for criminal intelligence purposes or for criminal investigative purposes—may have differences. With regard to criminal intelligence, information should be assessed to determine its validity and reliability, and products produced as a result of this information should include proper caveats. In some instances, it may be difficult to determine the validity of information obtained from a social media site (e.g., a citizen submits a tip about a video posted on YouTube depicting a robbery); however, that information may still be considered a potentially valid tip and should be documented as such.

In the case of a criminal investigation, information obtained from a social media site should be further evaluated to ensure that the information is authentic. For example, a video posted on YouTube shows individuals allegedly robbing a convenience store; law enforcement personnel should obtain a subpoena to determine what IP address was used to upload the video and identify to whom the IP address is registered. Information obtained from social media sites can be a valuable tool; however, comprehensive evaluation and authentication are crucial to ensure the reliability and validity of the information and ensure proper caveats are included, as necessary.

Case law has recently been established regarding authentication of information obtained by law enforcement. In *Griffin v. Maryland*, 2011 Md. LEXIS 226 (Md. 2011), the appeals court ruled that MySpace pages were erroneously admitted into evidence because they had not been properly authenticated. The trial court admitted the postings based on a police officer's testimony that the picture in the profile was of the purported owner and that they had the same location and date of birth. The picture, location, and birth date did not constitute sufficient "distinctive characteristics" to properly authenticate the MySpace printouts of the profile and posting because of the possibility that someone else could have made the profile or had access to it to make the posting. The court stated that there are different concerns when authenticating printouts from social media sites that go beyond the authentication concerns of e-mails, Internet chats, and text messages. Some suggested approaches to the social media authentication issue include an admission by the purported profile owner that it is his or her profile and he or she made the postings in question, a search of the person's computer and Internet history that links the subject to the profile or post, or information obtained directly from the social media site that identifies the person as the profile's owner and the individual with control over it, possibly including IP address identification information. This case demonstrates the need to validate information obtained from social media sites. ***As a source of information for lead development and follow-up, social media can be a valuable tool, but law enforcement personnel should always authenticate and validate any information captured from a social media Web site.***

**Action:** A social media policy should articulate that any information obtained from social media sites be evaluated to determine accuracy, validity, and/or authenticity. Social media interaction and usage are based on user uploads and updates and therefore should not serve as a primary/sole source for information gathering and verification. As with all sources of information, independent validation is important to determine accuracy and, more important, to protect individuals

<sup>14</sup> See *Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies* for additional information on law enforcement's role regarding First Amendment-protected events.

from being incorrectly identified, possibly leading to privacy violations and/or other inappropriate actions. Agencies may also refer to other policies and procedures related to criminal intelligence and investigative activities (and sources of information) as a part of the evaluation and authentication processes of information obtained from social media sites.

## ELEMENT 5

### SPECIFY THE DOCUMENTATION, STORAGE, AND RETENTION REQUIREMENTS RELATED TO INFORMATION OBTAINED FROM SOCIAL MEDIA RESOURCES.

**Background:** Based on the purpose for gathering information via social media resources (e.g., intelligence development, analysis assessment, or criminal investigations), agencies should identify the storage and retention requirements (why and for how long this type of information should be retained).<sup>15</sup> For criminal intelligence development and products, agencies may reference the storage and retention requirements identified in 28 CFR Part 23. For the documentation, storage, and retention requirements of information obtained from social media sites that is being utilized for a criminal investigation, agencies should refer to their investigative policies and procedures (and applicable laws and regulations).

If personally identifiable information (PII) (such as a name, a date of birth, or a picture) is identified and collected from social media sites, agencies should be sensitive to the documentation and retention of this information. If the information is part of criminal intelligence development, it is recommended that the tenets of 28 CFR Part 23 be followed; if the information is part of a criminal investigation, it is recommended that agency policy and procedures related to the dissemination of investigative information be referenced.

The documentation of this type of information should specify the purpose of the information use (regardless of the source of information), what information was collected (photos, status updates, friends), when the information was accessed and/or collected, where the information was accessed (identify the Web site), and how the information was collected (open search, nongovernmental IP address, undercover identity, etc.). Copies of the information obtained from the sites should also be documented. Additionally, as law enforcement personnel access social media sites, the reason for the use of the information obtained and the site utilized should be specified in the case or intelligence file.

For analysis assessments, the storage and retention period will be contingent on the assessment findings and whether a valid law enforcement purpose was identified. For example, a local law enforcement agency sends a request for information to the state fusion center to determine whether there are any threats or potential criminal activity associated with an upcoming demonstration. The fusion center creates an awareness assessment and references information obtained from social media resources that articulates that there are no threats identified. Further, the demonstration was peaceful, with no arrests. No potential criminal predicate or criminal nexus was identified either in the assessment itself or during the event, and therefore there is no articulable reason to store the information that was obtained as part of the analysis assessment.

For intelligence development purposes, the requirements of 28 CFR Part 23 should be followed regarding storage and retention of all information, whether collected from social media sites or other information sources. Though not all intelligence systems are required to adhere to 28 CFR Part 23, it has become a de facto national standard,<sup>16</sup> and as such, agencies are strongly encouraged to incorporate the tenets of this regulation into their policies and procedures regarding all criminal intelligence-related information.

<sup>15</sup> For additional information on file guidelines for criminal intelligence, please refer to the LEIU *Criminal Intelligence File Guidelines*, [http://it.ojp.gov/documents/ncisp/criminal\\_intel\\_file\\_guidelines.pdf](http://it.ojp.gov/documents/ncisp/criminal_intel_file_guidelines.pdf).

<sup>16</sup> See the *National Criminal Intelligence Sharing Plan*, Recommendation 9, [http://it.ojp.gov/documents/NCISP\\_Plan.pdf](http://it.ojp.gov/documents/NCISP_Plan.pdf).

If information from a social media site was gathered as part of a criminal investigation—such as a photo, identification of associates, or other PII—law enforcement personnel should adhere to agency policies and procedures regarding the documentation and storage of such information, carefully noting when and where the information was gathered.<sup>17</sup> A policy should also address the need to print or record the information gathered from the site to include in the case file for evidentiary purposes, due to the ease of changing social media information (users deleting information, changing their settings, etc.).

**Action:** The documentation, storage, and retention requirements for information obtained from social media resources should be articulated and defined in a social media policy. This section of the policy should be comparable to other investigative and/or intelligence policies regarding information documentation, storage, and retention.

## ELEMENT 6

### IDENTIFY THE REASONS AND PURPOSE, IF ANY, FOR OFF-DUTY PERSONNEL TO USE SOCIAL MEDIA INFORMATION IN CONNECTION WITH THEIR LAW ENFORCEMENT RESPONSIBILITIES, AS WELL AS HOW AND WHEN PERSONAL EQUIPMENT MAY BE UTILIZED FOR AN AUTHORIZED LAW ENFORCEMENT PURPOSE.

**Background:** The ease and accessibility of social media resources (including the use of applications [or apps] for smartphones and tablet computers) may affect how law enforcement personnel access social media when off duty,<sup>18</sup> as well as the use of personal equipment and personal accounts for official agency purposes. The information that is collected may result in criminal intelligence or lead to an active investigation; therefore, it is important to include a provision in the social media policy to address using information from social media sites for a law enforcement purpose by off-duty personnel and using nonagency equipment for official law enforcement purposes. With greater access to information through social media sites, it may be easier to identify criminal subjects and/or criminal activity, but it is also imperative to identify approved uses and access to the information.

For example, a law enforcement officer is off duty and is posting an update on his Twitter page. As part of his accessing Twitter on his personal computer, he notices a trending topic for his city about a robbery at a jewelry store. The agency's social media policy might require that the officer report this issue to dispatch and conduct a follow-up field incident report, documenting what he viewed, the site where he viewed the information, when he viewed it, and any action based on the information. In another example, an analyst is viewing her friends' status updates on Google+ and notices one friend expressing outrage at recent government policies (the friend does not make any threats, just articulates dissatisfaction). This posting is part of her friend's First Amendment right to free speech, and therefore no law enforcement documentation or other action should take place.

In another example, an intelligence officer who is focused on gang-related crime uses his personal Twitter account to "follow" a subject-matter expert (SME) in the field of gang identification and trends, as authorized in the agency's policy, which includes the provision for law enforcement officers to access social media sites, via personal accounts, as a part of their authorized law enforcement mission. The officer regularly updates his supervisor and intelligence unit members of trends identified by the SME and how these trends may be carried out in the jurisdiction.

Because of the widespread use of social media, agency policy must articulate when and how it is acceptable for off-duty personnel to use information from social media sites as part of their law enforcement mission. Law enforcement personnel

<sup>17</sup> It is important to note that the gathering of information from a social media site may be the result of a court-ordered lawful intercept. As such, there may be specific instructions regarding the gathering and storage of information.

<sup>18</sup> The IACP's Center for Social Media identifies five key policy considerations for agency policies regarding the use of social media, including the use of social media for personal use. See <http://www.iacpsocialmedia.org/GettingStarted/PolicyDevelopment.aspx>.

must adhere to law enforcement principles, whether on duty or at home surfing the Internet for a law enforcement purpose.

**Action:** A policy that addresses social media information should specify whether or not off-duty personnel may, as a part of an authorized law enforcement purpose, access social media sites and the reason(s) (if any) and requirements for access. If authorized, the policy should address the parameters in regards to accessing information that is viewed and gathered by off-duty personnel (for an authorized purpose), restrictions on the use of work equipment and/or personal equipment in an official law enforcement capacity while off-duty, and how to document and report the information that is gathered from the social media site.<sup>19</sup>

The policy should also specify whether or not law enforcement personnel may, when carrying out their authorized law enforcement mission and function, use personal equipment (including personal accounts) to access information via social media sites and the reason(s) and requirements associated with the use of personal equipment for this purpose. If the policy indicates that it is acceptable to use personal equipment for official agency purposes, then the policy should also direct personnel to document how information was obtained, the type of information obtained, the reason the information was obtained, and any follow-up action.

## ELEMENT 7 IDENTIFY DISSEMINATION PROCEDURES FOR CRIMINAL INTELLIGENCE AND INVESTIGATIVE PRODUCTS THAT CONTAIN INFORMATION OBTAINED FROM SOCIAL MEDIA SITES, INCLUDING APPROPRIATE LIMITATIONS ON THE DISSEMINATION OF PERSONALLY IDENTIFIABLE INFORMATION.

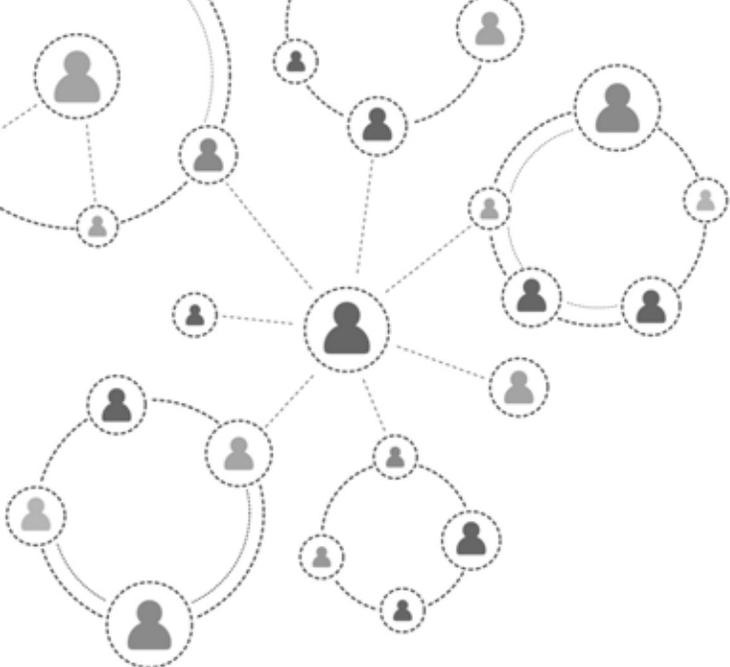
**Background:** Because of the open nature of many types of information obtained from social media sites, it is important to articulate dissemination procedures of products, reports, and requests for information that include information from social media sites.<sup>20</sup>

Additionally, the use of social media sites that focus on advocating greater information sharing among law enforcement agencies and personnel should be addressed in a policy. These sites offer greater access and information sharing capabilities; however, sharing any type of law enforcement information should be limited to nationally recognized sensitive but unclassified (SBU) networks (e.g., Regional Information Sharing Systems® [RISS], Law Enforcement Online [LEO], Homeland Security Information Network [HSIN]) and not social media/open source, commercially developed platforms.

**Action:** A social media policy should address dissemination protocols (who to disseminate to, timeline restrictions, how to disseminate information) for law enforcement reports, products, bulletins, and other types of information that may include information obtained from social media sites (and contain criminal intelligence information, criminal investigative information, and other information containing PII). Additionally, because of the sensitive nature of this type of information, the policy should address the incorporation of a review from a privacy officer and/or general counsel when disseminating products that include information from a social media site (including biographical information, photos, locations of subjects, etc.). A policy should also address dissemination mechanisms, such as using secure e-mail and SBU systems (not open source systems) to share criminal intelligence versus the use of social media sites to post bulletins to educate the public about criminal activity in the community.

<sup>19</sup> The IACP's Center for Social Media further addresses employee personal use of social media.

<sup>20</sup> For example, the validity and reliability of PII (e.g., photos, videos, and biographical information on a subject) that was obtained from social media sites may be unknown.



## CONCLUSION

Social media sites and resources may be a helpful tool for law enforcement personnel in the prevention, identification, investigation, and prosecution of crimes. Though social media sites are a relatively new resource for law enforcement, the same principles that govern all law enforcement activities should be adhered to as personnel access, view, collect, use, store, retain, and disseminate information from these types of sites; the same procedures and prohibitions that are placed on law enforcement officers when patrolling the community or conducting an investigation should be in place when law enforcement personnel utilize social media as a part of their public safety function.

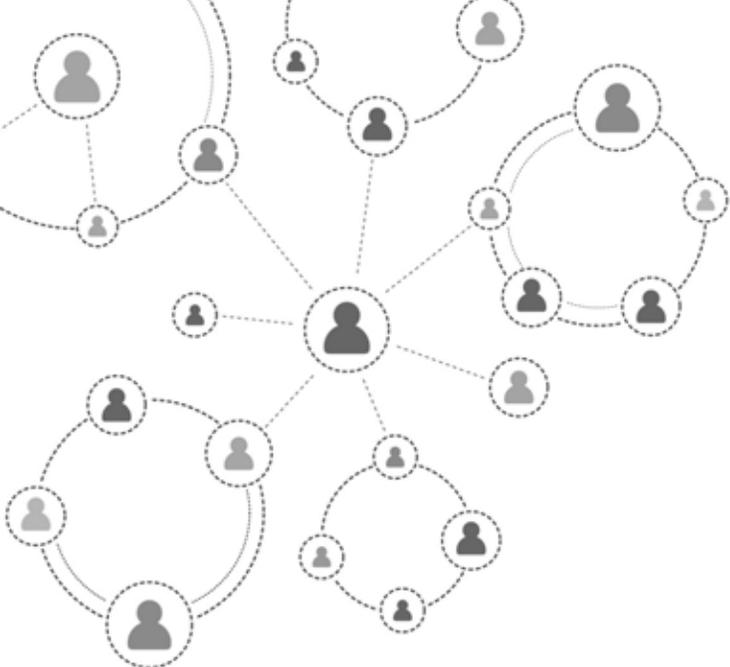
As with other law enforcement tools—such as uniform patrol, undercover activities, and search warrants—it is important to have a policy that articulates the how, when, and why of accessing, viewing, collecting, using, storing, and disseminating information obtained from social media sites, highlighting the privacy, civil rights, and civil liberties protections that are in place, regardless of the information source.

---

*Though social media sites are a relatively new resource for law enforcement, the same principles that govern all law enforcement activities should be adhered to as personnel access, view, collect, use, store, retain, and disseminate information from these types of sites.*

---





## APPENDIX A—CASES AND AUTHORITIES



These cases and authorities were relied on in the construction of the *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations* document. While these may be persuasive, it is always prudent to have agency legal counsel examine them in light of the controlling legal authorities in your jurisdiction.

### FOURTH AMENDMENT PRIVACY LAW AND THE INTERNET

**Expectation of Privacy in Internet Communications**, 92 A.L.R.5th 15, contains a good summary of current law regarding many forms of Internet communication, including

e-mail messages and inboxes, chat rooms, Web site content, and social-networking sites. Many cases cited within are summarized below.

***Smith v. Maryland***, 442 U.S. 735 (1979), forms the basis of the “third-party exposure” doctrine of electronic privacy law. In *Smith*, the government used pen register technology to record the numbers dialed out from a certain phone number. This information was used to convict the defendant of robbery. The defendant challenged the use of the pen register as an illegal search under the Fourth Amendment. The court ruled that the defendant did not have a reasonable expectation of privacy in the phone record information because the information was automatically turned over to a third party, the phone company. Even if the defendant had an expectation of privacy in the numbers dialed, it was not one society recognized as reasonable—therefore, there was no Fourth Amendment violation. This case has been analogized to Internet subscriber information, such as account existence and information on who the registered user of the account is because this information is automatically exposed to a third party, the Internet service provider.

**United States v. Jones**, 132 S. Ct. 945 (2012), is a case involving law enforcement's placement of a Global Positioning System (GPS) device on a subject's car and use of the device to monitor the vehicle's movement on public streets for a four-week period (which extended beyond the period of time and place authorized by a search warrant). The Supreme Court Justices unanimously agreed that use of the GPS device constituted a search within the meaning of the Fourth Amendment. The majority explained that a physical intrusion into a constitutionally protected area, coupled with an attempt to obtain information, can constitute a violation of the Fourth Amendment based upon a theory of common law trespass. The majority explained that "the use of longer-term GPS monitoring in investigations of most offenses impinges on expectations of privacy." Additionally, in a separate opinion, one justice suggested that it may be time to rethink all police use of tracking technology, not just long-term GPS, reasoning that "GPS monitoring generates a precise, comprehensive record of a person's public movement that reflects a wealth of detail about her familial, political, religious, and sexual associations.... The government can store such records and efficiently mine them for years to come." The reasoning expressed by the justices in *Jones* could have broad implications for law enforcement use of social media in such areas as law enforcement personnel access to information from social media sites and the determination as to whether the social media user has a reasonable expectation of privacy due to privacy controls set up by the user.

**United States v. Kennedy**, 81 F. Supp. 2d 1103 (D. Kan. 2000). Relying on *Smith* (above), the District Court of Kansas ruled that the defendant did not have a reasonable expectation of privacy in information knowingly turned over to his Internet service provider, including Internet subscriber information and information associated with his Internet Protocol (IP) address. Divulgence of this information to law enforcement by Road Runner cable did not violate defendant's Fourth Amendment rights. See also **United States v. Ohnesorge**, 60 M.J. 946 (N.M. Ct. Crim. App. 2005) (the court did not abuse its discretion in refusing to suppress Internet service provider information, specifically subscription information to a news and file access sharing Web site obtained without a warrant. The defendant did not have a reasonable expectation of privacy in the information; the subscription information was never confidential, and the defendant acknowledged that the information could be shared in the terms of service agreement with the site).

## SOCIAL MEDIA AND PRIVACY LAW

Nathan Petrashek Comment, "**The Fourth Amendment and the Brave New World of Online Social Networking**," 93 Marq. L. Rev. 1495 (summer 2010). This law review article provides a thorough background on social-networking sites and how the two largest, MySpace and Facebook, operate. A current case law summary is provided as well as an explanation of different privacy doctrines and how they can be applied to the social media setting.

**Katz v. United States**, 389 U.S. 347 (1967), provides the foundation for most federal court privacy rulings and doctrines. *Katz* moved away from previous Supreme Court privacy jurisprudence in holding that the Fourth Amendment protects people and not places, overruling the previous "trespass" doctrine of Fourth Amendment protection. Fourth Amendment considerations no longer require a physical invasion or trespass. In this case, police eavesdropped on private conversations from a public telephone booth, and the court found that even though no physical invasion of the phone booth occurred, this was not necessary to constitute a search for purposes of the Fourth Amendment. Police violated the defendant's Fourth Amendment privacy interests by listening to the content of the conversations without a proper warrant. *Katz* established a two-prong test to determine whether the Fourth Amendment is implicated and a search has occurred. If a person, like *Katz*, has manifested an intent to make the information private *and* society accepts that expectation of privacy as reasonable, then that privacy expectation cannot be violated without following Fourth Amendment warrant requirements.

**Minnesota v. Olson**, 495 U.S. 91 (1990), further explained the application of *Katz* and the two-prong expectation of privacy test. As an overnight guest, the defendant did have an expectation of privacy in the dwelling, and that expectation is recognized by society as reasonable.

**Courtright v. Madigan**, 2009 U.S. Dist. LEXIS 102544 (S.D. Ill. 2009). The defendant was convicted of three separate offenses of producing, possessing, and receipt of child pornography by a repeat offender. The case initiated through a subpoena served on MySpace.com by the Illinois Attorney General's Office in an effort to learn whether any registered sex offenders were using that site. Upon learning the defendant had a MySpace account, investigators took further steps to discover his IP address and learned that this address had offered pornographic images on the file-sharing site Limewire. These discoveries formed the basis of a warrant that uncovered evidence that was used to convict the defendant. The defendant argued that the initial information gathered from MySpace regarding his account violated his protection against unreasonable searches and seizures under the Fourth Amendment. For other procedural reasons, the defendant's appeal was denied, but the court addressed the search issue and, relying on multiple other courts, held that the defendant had no privacy expectation in Internet subscriber information based on the third-party exposure doctrine. The defendant had no expectation of privacy in the fact that his MySpace account existed, so the request for information on that matter did not violate his Fourth Amendment rights.

**Commonwealth v. Proetto**, 771 A.2d 823 (Pa. Super. Ct. 2001). In *Proetto*, the defendant was brought to the attention of police after a 15-year-old female who had been contacted by the defendant in a public chat room turned over logs of chats that contained explicit information and solicited sexual activity from the underage girl. Police asked the informant to cease communication with the defendant but inform them when he was online again. When police were informed that the defendant was online, they entered the chat room the defendant was in, posing as a 15-year-old girl. The defendant made sexually suggestive comments to the "underage female," which law enforcement officers logged. The defendant challenged use of the chat room logs and e-mail messages under the Fourth Amendment and Pennsylvania Wiretap Act. First, for the communication forwarded to police from the underage informant, the court analogized the e-mail and chat communications to letters and found a limited privacy right. As with letters, the expectation of privacy in the information was reasonable until the intended recipient received the information. After that, because the information could easily be forwarded to others, there remains no reasonable expectation of privacy; therefore, there was no Fourth Amendment violation. For the chats, the defendant did not know exactly whom he was speaking to so he did not have a reasonable expectation of privacy. Communications made directly to the undercover officer survive Fourth Amendment challenges under the same reasoning in that the defendant has only limited privacy interests in e-mail communications. Because the defendant communicated freely with the undercover officer and could not verify the officer's identity, he had no reasonable expectation of privacy in the chat communications. The fact that the officer did not identify himself as law enforcement is of no consequence. The Pennsylvania Wiretap Act was not violated because the informant and the police were both the intended recipients and parties to the communication and recorded the messages concurrently with the communication. For similar case law, see **United States v. Maxwell**, 45 M.J. 406 (C.A.A.F. 1996) (no expectation of privacy found in e-mail communications in child pornography case); **United States v. Charbonneau**, 979 F. Supp. 1177 (S.D. Ohio 1997) (explaining chat room and privacy expectations around Internet service providers, finding no reasonable expectation of privacy); and **Ohio v. Turner**, 156 Ohio App. 3d 177 (Ohio Ct. App. 2004) (no expectation of privacy in chat room conversations with undercover agent posing as underage boy).

**Guest v. Leis**, 255 F.3d 325 (6th Cir. 2001). After receiving a tip regarding online obscenity, police began investigating two electronic bulletin board systems. Police assumed an undercover identity to receive a password to the bulletin board, which enabled them to send e-mails to members, post messages, and share pictures, among other things. After viewing pornographic activity, the police obtained subscriber information from the bulletin boards. Defendants filed a class-

action suit citing violation of their Fourth Amendment rights when the police accessed subscriber information for the bulletin boards, which included the subscribers' name, address, birth date, and password. The court concluded that, like other information provided to a third party, this information was not protected by the Fourth Amendment and there is no reasonable expectation of privacy attached to it.

**J.S. v. Bethlehem Area School District**, 757 A.2d 412 (Pa. Commw. Ct. 2000), involved a student's off-campus Web site postings. A student created a Web site with derogatory comments about a teacher and the school administration. As a result of these postings, the student was expelled. The court found that the school did not violate the student's privacy rights when accessing the materials posted on the Web site. The Web site was not password-protected and was available to anyone that came across it on the Internet. The court reasoned that once material is published on a Web site, it is open to the public. If the creator does not take any steps to protect the Web site content and make it private, no expectation of privacy can be said to exist. See also **Konop v. Hawaiian Airlines, Inc.**, 236 F.3d 1035 (9th Cir. 2001) (employer did not violate employee's privacy rights by accessing public, unprotected Web site postings. *Konop* held there is no expectation of privacy in information posted to public Web sites).

**United States v. Drew**, 259 F.R.D. 449 (C.D. Cal. 2009). This case involved use of a fake MySpace profile that was created and used in violation of the Web site's terms of service contract agreed to by all users. The Central District of California's court found that in some instances, the violation of a terms of service agreement could constitute a misdemeanor offense under the Computer Fraud and Abuse Act. The court vacated the conviction, however, because the statute did not pass the constitutionality void for vagueness test based on the absence of guidelines in the statutory scheme to guide law enforcement and an actual notice requirement. Although involving civilian use of social media, the reasoning and analysis could be useful to guide law enforcement officers who are using social media and fake profiles in undercover investigations.

## DOCUMENTING SOCIAL MEDIA DURING AN INVESTIGATION

Todd G. Shipley, **Collecting Legally Defensible Online Evidence: Creating a Standard Framework for Internet Forensic Investigations**. Vere Software Investigative Tools. December 2001. Available at <http://veresoftware.com/uploads/CollectingLegallyDefensibleOnlineEvidence.pdf>. Last accessed June 9, 2011. This document explains the difference between Internet evidence gathering and traditional computer-based evidence gathering. The collection, preservation, and presentation technique for gathering Internet evidence is explained in the document. References to outside sources and summaries of some documentation techniques are also included.

**Kyllo v. United States**, 533 U.S. 27 (2001), establishes the Supreme Court rule on advanced technology use in searches. In *Kyllo*, the police suspected the defendant of growing marijuana inside his residence. They utilized thermal imaging equipment to "peer through" the walls of the home and determine the defendant was growing marijuana. The court of appeals upheld the search on the basis that the defendant did not make any effort to conceal the heat emanating from his home and therefore did not have a reasonable expectation of privacy under the Fourth Amendment. The Supreme Court reversed, holding that the thermal imaging infiltrated the home and did constitute a search under the Fourth Amendment. The Supreme Court ruled that it was a search in violation of the Fourth Amendment because the thermal imaging gained information, through technology not generally used by the public, that could not have otherwise been gained without physical intrusion of the home, a constitutionally protected area without a warrant.

**Hubbard v. MySpace, Inc.**, 2011 U.S. Dist. LEXIS 58249 (S.D. N.Y. 2011), establishes that social-networking sites, such as MySpace, can provide account user information, IP address information, IP address use date and time logs, and contents of the user's private messages and sent-message folders to law enforcement in response to a valid subpoena or warrant under the Electronic Communications Privacy Act.

## AUTHENTICATING SOCIAL MEDIA EVIDENCE

**Authentication of Electronically Stored Evidence, Including Text Messages and E-Mail**, 34 A.L.R.6th 253. This document outlines the state of case law regarding authentication of various electronic communications, including text messages, e-mails, chat and instant messages, and others. This source provides general background on authentication issues with electronically stored communications; however, the agency or office will need to check the jurisdiction's specific requirements.

**Griffin v. Maryland**, 2011 Md. LEXIS 226 (Md. 2011). In a case involving evidence of witness intimidation obtained from a MySpace profile purported to be that of the defendant's girlfriend, the court relied upon officer testimony. Based on the picture on the profile, the defendant's girlfriend's birthday and profile birthday being the same, and the location listed on the profile, it was determined that this was the profile of the defendant's girlfriend. The trial court authenticated the evidence solely on officer testimony regarding the profile's information and admitted it into evidence. On appeal, the court found error because no extrinsic evidence was used to authenticate the profile or posting. The court reasoned that the picture, location, and birth date alone are not sufficient "distinctive characteristics" to authenticate a MySpace profile printout because someone else could have created the page and made the posting.

**Lorraine v. Markel American Insurance Company**, 241 F.R.D. 534 (D. Md. 2007), outlines the various ways digital and Internet-based evidence can be authenticated in court. The opinion analyzes the applicable federal rules of evidence and how they can be applied to electronically stored evidence. The opinion provides a good guide for law enforcement with respect to the type of information needed for the authentication of Internet-based evidence. Specifically, the opinion explores identifying and authenticating characteristics of e-mail messages, Internet Web site postings, text messages and chat room content, computer-stored and -generated data, and digital photographs. Citations to cases in other jurisdictions explaining electronic evidence authentication are also included.

## SUCCESSFUL USE OF SOCIAL MEDIA EVIDENCE IN INVESTIGATIONS AND TRIALS

**U.S. v. Underwood**, 2010 U.S. Dist. LEXIS 134543 (W.D. Ky. 2010), is a case regarding child pornography and enticing a minor charges. The charges originated from an undercover police investigation conducted online with an officer posing as a 13-year-old boy. The investigation was initiated after an anonymous caller to the police tip line reported a possible pedophile operating on the MySpace social-networking Web site. The police officer then created an undercover profile purporting to be a 13-year-old boy and sent a friend request to the defendant. The defendant engaged the undercover officer in communication on the MySpace and Yahoo! Web sites, with much of the conversation having a sexual nature. Based on this initial investigation, subpoenas were served on the Web sites and various Internet service providers, which resulted in identification of the defendant as the various accounts' holder, the IP addresses associated with those accounts, and his home address. This was used to apply for a search warrant of the defendant's house. Evidence was suppressed because the warrant issued was for evidence of child pornography, while the affidavit accompanying the application referred only to the crime of enticing a minor. In this case, redaction of the warrant and partial suppression were not an adequate remedy; however, probable cause had been established by the social media evidence for a warrant to search for evidence of enticing a minor. If not for the discrepancy in the request to search for evidence and a warrant issued for child pornography crimes and the probable cause listed in the application for enticing a minor, the social media evidence would have provided valid probable cause to issue a warrant. See also **U.S. v. Lee**, 603 F.3d 904 (11th Cir. 2010) (evidence from a social-networking site was sufficient to uphold convictions of attempted enticement of a minor, attempted production of child pornography, and knowing receipt of child pornography even though communications through the site were with an adult and the children were fictitious. Evidence consisted of multiple online conversations between an undercover postal inspector and the defendant and one recorded phone call); **U.S. v. Schene**, 543 F.3d 627 (10th Cir. 2008) (social media

investigation evidence and computer account activity used to confirm that the defendant was in fact the person at the IP address who received child pornography).

**In the Interest of F.P.**, 878 A.2d 91 (Pa. Super. Ct. 2005), is a case involving a juvenile delinquency charge resulting from an assault. Evidence used to support a finding of delinquency included instant messages sent from the delinquent juvenile to the victim. The juvenile challenged their admission based on improper authentication because no evidence of their source from the Internet service provider or by a computer forensics expert was provided. The court upheld the finding of delinquency and ruled the authentication was proper based on the circumstantial evidence provided at the adjudication hearing. The basis for authenticating the instant messages rested on the facts that the juvenile identified himself with his first name in the conversations, made accusations in the conversations that were consistent with testimony of other witnesses, and referenced the victim reporting the threats to school officials. Moreover, the character of the messages and conversations was consistent with other testimony regarding the juvenile's feelings and actions towards the victim. These circumstantial facts were sufficient to authenticate the instant messages as coming from the delinquent juvenile.

**A.B. v. Indiana**, 885 N.E. 2d 1223 (Ind. 2008), involves alleged threats made by a student against her principal on the MySpace social-networking site. The opinion does not address authentication issues but does provide an overview on how the MySpace site functions and explains the difference between "public" and "private" profiles, groups, and postings. Authentication issues were resolved by student testimony and permission to access the MySpace postings from their profile, which was "friends" with the appellant student's admitted profile.

**Munoz v. State**, 2009 Tex. App. LEXIS 256 (Tex. App. 2009). The defendant challenged, among other things, a criminal street gang enhancement charge. During the course of an assault trial resulting from a drive-by shooting incident, an investigator with the district attorney's office testified as to how to identify gang members and that based on his investigation, the defendant was a gang member. Several MySpace pictures the investigator used to form his opinion on gang involvement were admitted into evidence. The investigator, who maintained a local gang database and was knowledgeable on local gang activity, provided testimony and evidence from his MySpace investigations of the defendant. This testimony, coupled with testimony from other witnesses and evidence recovered from the defendant's room, formed a legally sufficient basis to convict the defendant on the criminal gang enhancement charge.

**People v. Chavez**, 2010 Cal. App. Unpub. LEXIS 6186 (Cal. Ct. App. 2010),<sup>21</sup> upheld information charging the defendant's involvement with a criminal street gang. An investigator from the district attorney's office was qualified as a gang expert at trial and testified to common characteristics of gang members and how to identify them. As part of the expert's conclusion that the defendant was an active gang member, the expert relied on a MySpace posting containing a picture of the defendant, the name of the gang, and the defendant's gang moniker. The MySpace evidence and testimony of the expert provided enough of a basis for the information to survive dismissal challenges. See also **People v. Corleone**, 2009 Cal. App. Unpub. LEXIS 3107 (Cal. Ct. App. 2009)<sup>22</sup> (stalking and criminal threat convictions upheld based on MySpace, e-mail, and text-message evidence); **People v. Abusharif**, 2011 Ill. App. Unpub. LEXIS 853 (Ill. App. Ct. 2011)<sup>23</sup> (trial court did not abuse discretion in admitting text message and MySpace message evidence in murder trial).

**U.S. v. McNamara-Harvey**, 2010 U.S. Dist. LEXIS 106141 (E. D. Pa. 2010). Anonymous tips that the defendant posted pro-Palestinian/anti-Israeli videos on his Facebook page, as well as personal admissions from the defendant to the Federal Bureau of Investigation (FBI) that he had posted disturbing and/or extremist videos, helped form the basis of a warrant for computer-based evidence of potential terroristic acts.

---

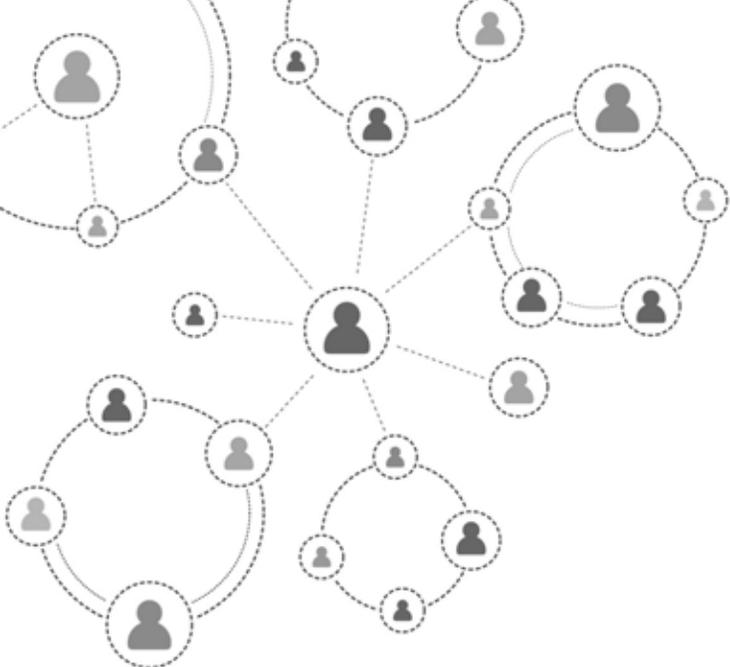
21 This is an unpublished opinion. Please check local court rules when relying on this opinion as authority.

22 See Footnote 21.

23 See Footnote 21.

**Griffin v. Maryland**, 2011 Md. LEXIS 226 (Md. 2011). The appeals court ruled that MySpace pages were erroneously admitted into evidence because they had not been properly authenticated. The trial court admitted the postings based on a police officer's testimony that the picture in the profile was of the purported owner and they had the same location and date of birth. The picture, location, and birth date did not constitute sufficient "distinctive characteristics" to properly authenticate the MySpace printouts of the profile and posting because of the possibility that someone else could have made the profile or had access to it to make the posting. The court stated that there are different concerns when authenticating printouts from social media sites that go beyond the authentication concerns of e-mails, Internet chats, and text messages. Some suggested approaches to the social media authentication issue include an admission of the purported profile owner that it is his or her profile and he/she made the postings in question, a search of the person's computer and Internet history that links the subject to the profile or post, or information obtained directly from the social media site that identifies the person as the profile's owner and individual with control over it, possibly including IP address identification information.





# APPENDIX B— GEORGIA BUREAU OF INVESTIGATION SOCIAL MEDIA POLICY

Georgia Bureau Of Investigation Investigative Division  
Directive 8-6-5

Title: Guidelines For The Use Of Social Media By The Investigative Division

Date: October 26, 2012

Reviewed: October 26, 2012

Authority: R. E. Andrews  
Deputy Director For Investigations

Page 1 of 12

Purpose: To establish guidelines for the use of social media in pre-employment background investigations, crime analysis and situational assessments, criminal intelligence development, and criminal investigations.

## DEFINITIONS

**Crime Analysis and Situational Assessment Reports**—Analytic activities to enable GBI to identify and understand trends, causes, and potential indicia of criminal activity, including terrorism.

**Criminal Intelligence Information**—Data which meets criminal intelligence collection criteria and which has been evaluated and determined to be relevant to the identification of criminal activity engaged in by individuals who or organizations which are reasonably suspected of involvement in criminal activity.

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

**Online Alias**—An online identity encompassing identifiers, such as name and date of birth, differing from the employee’s actual identifiers, that uses a nongovernmental Internet Protocol address. Online alias may be used to monitor activity on social media websites or to engage in authorized online undercover activity.

**Online Undercover Activity**—The utilization of an online alias to engage in interactions with a person via social media sites that may or may not be in the public domain (i.e. “friending a person on Facebook”).

**Public Domain**—Any Internet resource that is open and available to anyone.

**Social Media**—A category of Internet-based resources that integrate user-generated content and user participation. This includes, but is not limited to, social media networking sites (Facebook, MySpace), micro blogging sites (Twitter), photo- and video-sharing sites (Flickr, YouTube), wikis (Wikipedia), blogs, and news sites (Digg, Reddit).

**Social Media Monitoring Tool**—A tool used to capture data and monitor social media sites by utilizing automated tools such as web crawlers and word search functions to make predictive analysis, develop trends, or collect information. Examples include Netbase, Twitterfall, Trackur, Tweetdeck, Socialmention, Socialpointer, and Plancast.

**Social Media Websites**—Sites which focus on building online communities of people who share interests and activities and/or exploring the interests and activities of others. Social media websites are further categorized by Internet-based resources that integrate user-generated content and user participation. This includes, but is not limited to, social networking sites (Facebook, MySpace), micro blogging sites (Twitter, Nixle), photo- and video-sharing sites (Flickr, YouTube), wikis (Wikipedia), blogs, and news sites (Digg, Reddit). The absence of an explicit reference to a specific social media website does not limit the application of this policy.

**Valid Law Enforcement Purpose**—A purpose for information/intelligence gathering development, or collection, use, retention, or sharing that furthers the authorized functions and activities of a law enforcement agency, which may include the prevention of crime, ensuring the safety of the public, furthering officer safety, and homeland and national security, while adhering to law and agency policy designed to protect the privacy, civil rights, and civil liberties of Americans.

## I. GENERAL

Social media may be a valuable investigative tool to detect and prevent criminal activity. Social media has been used for community outreach events such as providing crime prevention tips, providing crime maps, and soliciting tips about unsolved crimes. Social media may also be used to make time sensitive notifications regarding special events, weather emergencies, or missing or endangered persons. While social media is a new resource for law enforcement, employees must adhere to this policy to protect individuals’ privacy, civil rights, and civil liberties and to prevent employee misconduct.

## II. UTILIZATION OF SOCIAL MEDIA

**A. Social media may be used by Investigative Division personnel for a valid law enforcement purpose. The following are valid law enforcement purposes:**

1. Pre-employment background investigations;
2. Crime analysis and situational assessment reports;
3. Criminal intelligence development; and
4. Criminal investigations.

- B. While on duty, employees will utilize social media, access social media websites, online aliases, and social media monitoring tools only for a valid law enforcement purpose. The utilization of an online alias or social media monitoring tool for personal use is prohibited and is considered employee misconduct.**
- C. Employees will only utilize social media to seek or retain information that:**
1. Is based upon a criminal predicate or threat to public safety; or
  2. Is based upon reasonable suspicion that an identifiable individual, regardless of citizenship or U.S. residency status, or organization has committed an identifiable criminal offense or is involved in or is planning criminal conduct or activity that presents a threat to any individual, the community, or the nation and the information is relevant to the criminal conduct or activity (criminal intelligence information); or
  3. Is relevant to the investigation and prosecution of suspected criminal incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime; or
  4. Is useful in crime analysis or situational assessment reports for the administration of criminal justice and public safety; or
  5. Is relevant to pre-employment background investigations.
- D. The GBI will not utilize social media to seek or retain information about:**
1. Individuals or organizations solely on the basis of their religious, political, social views or activities; or
  2. An individual's participation in a particular non-criminal organization or lawful event; or
  3. An individual's race, ethnicity, citizenship, place of origin, disability, gender, or sexual orientation unless such information is relevant to the individual's criminal conduct or activity or if required to identify the individual; or
  4. An individual's age other than to determine if someone is a minor.
- E. The GBI will not directly or indirectly receive, seek, accept, or retain information from:**
1. An individual or nongovernmental information provider who may or may not receive a fee or benefit for providing the information if there is reason to believe that the information provider is legally prohibited from obtaining or disclosing the information; or
  2. A source that used prohibited means to gather the information.

### **III. AUTHORIZATION TO ACCESS SOCIAL MEDIA WEBSITES**

This section addresses the authorization necessary to utilize social media and access social media websites for crime analysis and situational awareness/assessment reports; intelligence development; and criminal investigations.

#### **A. Public Domain**

No authorization is necessary for general research, topical information or other law enforcement uses that do not require the acquisition of an online alias.

#### **B. Online Alias**

An online alias may only be used to seek or retain information that:

1. Is based upon a criminal predicate or threat to public safety; or

2. Is based upon reasonable suspicion that an identifiable individual, regardless of citizenship or U.S. residency status, or organization has committed a criminal offense or is involved in or is planning criminal conduct or activity that presents a threat to any individual, the community, or the nation and the information is relevant to the criminal conduct or activity; or
3. Is relevant to the investigation and prosecution of suspected criminal incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime; or
4. Is useful in crime analysis or situational assessment reports for the administration of criminal justice and public safety.

### **C. Authorization for Online Aliases**

Sworn agents or criminal intelligence analysts must submit a request for an online alias. No other Investigative Division personnel are authorized to submit requests for an online alias or to use an online alias in the performance of their official duties.

The request must contain the following information:

1. Purpose for the request (i.e. type of investigative activity);
2. Username;
3. Identifiers and pedigree to be utilized for the online alias, such as email address, username and date of birth. Do not include password(s) for online aliases and ensure password(s) are secured at all times; and
4. Photograph to be used with online alias, if applicable.

The work unit supervisor must evaluate the request to determine whether an online alias would serve a valid law enforcement purpose. The work unit supervisor must maintain the requests for online alias and their status (approved/denied) for two years from the date of deactivation of the online alias.

Investigative Division personnel with an approved online alias may use their online alias to make false representations in concealment of personal identity in order to establish social media accounts (i.e. a Facebook account). The establishment of a social media account with an approved online alias must be documented.

### **D. Authorization for Online Undercover Activity**

1. A sworn agent who has an authorized online alias may also request authorization to engage in online undercover activity. Only agents will be authorized to engage in online undercover activity utilizing the online alias.
2. Online undercover activity occurs when the agent utilizing the online alias interacts with a person via social media. Online undercover operations will only be utilized 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).
3. Employees must submit a request to engage in online undercover activity. The request must contain the following information:
  - a. Online alias(es) to be used in the online undercover activity;
  - b. Social media accounts utilized;
  - c. Valid law enforcement purpose; and
  - d. Anticipated duration for the online undercover activity.

4. The work unit supervisor must evaluate the request to determine whether online undercover activity is appropriate. If the request is approved, the authorization must be maintained in the file containing the record of the online undercover activity.
5. In situations involving exigent circumstances, the work unit supervisor may provide verbal authorization for online undercover activity. The work unit supervisor should provide written documentation of the request, the exigent circumstances, and the circumstances of the verbal authorization as soon as practical.
6. A record will be maintained of all online undercover activity.
7. Once authorized to engage in online undercover activity, the agent should utilize the appropriate deconfliction system.
8. All approved online undercover activity requests will be reviewed monthly by the work unit supervisor to ensure continued need for the online undercover activity. Approved online undercover activity that does not provide information regarding a valid law enforcement purpose within thirty (30) days will be discontinued.
9. A summary will be placed in the file indicating the date of termination of the online undercover activity. The online alias may be maintained if it is anticipated that it will be utilized again.

#### **IV. AUTHORIZATION TO UTILIZE SOCIAL MEDIA MONITORING TOOLS**

- A. Prior to utilizing a social media monitoring tool, the work unit supervisor will submit a request through the chain of command to the Deputy Director for Investigations for authorization to use the social media monitoring tool. The social media monitoring tool may be utilized in criminal investigations; criminal intelligence development; and crime analysis and situational assessment reports (e.g. during sporting events, demonstrations or other large gatherings that require a law enforcement presence to ensure the safety of the public). The request must contain the following:**
  1. A description of the social media monitoring tool;
  2. Its purpose and intended use;
  3. The social media websites the tool will access;
  4. Whether the tool is accessing information in the public domain or information protected by privacy settings; and
  5. Whether information will be retained by the GBI and if so, the applicable retention period for such information.
- B. The request must be reviewed by the GBI Privacy Officer prior to approval.**
- C. In exigent circumstances, the work unit supervisor may obtain verbal authorization to utilize the social media monitoring tool and provide written documentation as soon as practical. The written documentation should include a description of the exigent circumstances and the verbal authorization, as well as the required information for the request.**
- D. If approved, the social media monitoring tool may be utilized for a period of ninety (90) days or, in the case of situational assessments such as an event or large gathering, until the conclusion of the law enforcement activity related to the event. After ninety (90) days, the work unit supervisor must submit a summary describing the law enforcement actions that resulted from the use of the social media monitoring tool.**

If continued use is needed, the summary may also contain a request to continue using the social media monitoring tool. The process to approve the request is the same as the original request.

## V. SOURCE RELIABILITY AND CONTENT VALIDITY

Information developed from social media sites should be corroborated using traditional investigative tools including interviews, verification of address, verification of internet protocol address information, or other lawful means.

## VI. DOCUMENTATION AND RETENTION

Other than crime analysis and situational assessment reports, all information obtained from social media websites shall be placed within a case file, suspicious activity report, or intelligence report. At no time should Investigative Division personnel maintain any social media files outside of these authorized files.

Crime analysis and situational assessment reports may be prepared for special events management, including First Amendment-protected activities. At the conclusion of the situation requiring the report or First Amendment-protected event where there was no criminal activity related to the information gathered, the information obtained from the social media monitoring tool will be retained for no more than fourteen (14) days. Information from the social media monitoring tool that does indicate a criminal nexus will be retained in an intelligence report, suspicious activity report, or case investigative file as directed by the State of Georgia retention schedule.

Information identified as criminal in nature that is obtained in the course of an investigation from a social media site will be collected and retained using screen shots, printouts of chat logs, copying uniform resource locators (URL's) for subpoena or investigatory purposes, or storing the information via secure digital means. When possible, employees will utilize investigative computer systems and software intended to record data from social media sites.

## VII. OFF DUTY CONDUCT

- A. An employee who becomes aware of potential criminal activity via the Internet while off duty shall contact their supervisor or CEACC if the activity involves a minor child or exigent circumstances to determine the best course of action.
- B. As soon as practical following awareness of the potential criminal activity, the employee should prepare detailed notes to document a complete description of the information observed and specifics as to the events that occurred or action taken.
- C. Employees shall act to preserve and maintain proper custody of images, texts, photographs, or other potential evidence.

## VIII. PERSONAL EQUIPMENT AND PERSONAL SOCIAL MEDIA WEBSITES AND PASSWORDS

Given the ease with which information can be gathered from public internet searches, tracking services, and other computer analytic technology, the use of employee's personal or family internet accounts, social media, or internet service for official GBI business is prohibited.

## IX. DISSEMINATION

Retention and dissemination of social media information will be the same as the type of file, whether a paper or electronic file, in which the information is located. For example, retention and dissemination of social media

information within an intelligence file will be treated in the same manner as an intelligence file. Information developed during the course of a criminal investigation will be located in the investigative case file and retained and disseminated in the same manner as the investigative case file.

## **X. EMPLOYMENT BACKGROUND INVESTIGATIONS**

As part of its employment background process, Investigative Division personnel will conduct a search of social media websites and profiles in the public domain regarding the applicant. Applicants will be notified that this search will be conducted. Applicants are not required to disclose passwords to social media sites or profiles to the GBI. In the event an applicant discloses their password, the GBI will not utilize the password to log into the applicant's social media site or profile. Employees will not search or attempt to gain access to private social media profiles.

All searches of applicant social media pages and profiles will only search information that is in the public domain. Online aliases will not be used to conduct employment background investigations.

Only criminal comments or images will be collected as part of the background investigatory process. Employees will not collect or maintain information about the political, religious, or social views, associations or activities of any individual or any group unless such information directly relates to criminal conduct or activity.

During the course of a background investigation, if a reference, supervisor, or colleague of the applicant provides negative information on the applicant related to a social media site, the agent will prepare an investigative summary outlining the information provided by the reference.

## **XI. SANCTIONS FOR MISUSE**

Any employee who violates the provisions of this directive will be subject to disciplinary action, up to and including termination.

## **XII. COMPLAINTS AND INFORMATION QUALITY ASSURANCE**

Employees will report violations or suspected violations of this directive to the Privacy Officer in accordance with the GBI Privacy Policy, Directive 7-6 Criminal Intelligence and Privacy Protections, Section VI (D).

Complaints from the public regarding information obtained from social media websites will be submitted to the Privacy Officer and handled in accordance with the GBI Privacy Policy. If the information is determined to be erroneous, the information will be corrected or deleted.

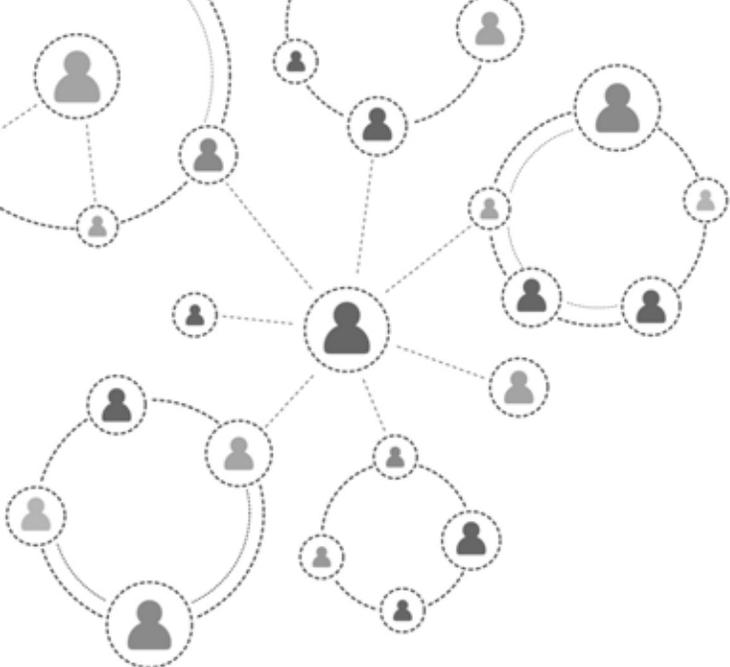
## **XIII. AUDIT**

As part of the GBI annual privacy audit, compliance with this directive will be verified by a GBI inspection team led by the Privacy Officer.

## **XIV. ANNUAL REVIEW**

The GBI Privacy Officer will review this directive at least annually and direct the updating of the policy and procedures as necessary.





# APPENDIX C— DUNWOODY POLICE DEPARTMENT SOCIAL MEDIA POLICY

## DUNWOODY POLICE DEPARTMENT STANDARD OPERATING PROCEDURE

Subject	Social Media
Effective Date	November 15, 2011
Sop #	A-50
Reference	Social Media Pages, Blogs, Twitter, Departmental Material, Agency And Personnel Electronic Devices
Special Instructions	Annual Review
Distribution	All Personnel
# Pages	4

### I. PURPOSE

The department endorses the use of social media to enhance communication, collaboration, and information exchange; streamline processes; and foster productivity. This policy establishes the department's position on the utility of social media, including management, administration, and oversight. This policy is intended to address social media in general, not a particular form of social media.

### II. POLICY

Social media provides a potentially valuable means of assisting the department and department personnel in meeting community outreach, problem-solving, investigative, crime prevention, and related goals of the department. This policy identifies potential uses that may be explored or expanded upon as directed by the Chief of Police. The personal use of social media can have a bearing on department personnel in their official capacity. As such, this policy provides information of a precautionary nature as well as prohibitions on the use of social media by department personnel.

### III. DEFINITIONS

**Blog**—A self-published commentary on a particular topic that may allow visitors to post responses, reactions, or comments. This term is short for "Web log."

**Page**—The specific portion of a social media website where content is displayed and managed by an individual or individuals.

**Post**—Content an individual shares on a social media site or the act of publishing content on a site.

**Profile**—Information that a user shares about himself or herself on a social networking site.

**Social Media**—A category of Internet-based resources that integrate user-generated content and user participation. This includes, but is not limited to, social networking sites (Facebook, MySpace), microblogging sites (Twitter, Nixle), photo- and video-sharing sites (Flicker, YouTube), wikis (Wikipedia), blogs, and news sites (Digg, Reddit).

**Social Networks**—Online platforms where users can create profiles, share information, and socialize with others user a range of techniques.

**Speech**—Expression or communication of thoughts or opinions in spoken words, in writing, by expressive conduct, symbolism, photographs, videotape, or related forms of communication.

**Electronic Communications**—Electronic Communications include, among other things, messages, images, data or any other information used in e-mail, instant messages, voice mail, fax machines, computers, personnel digital assistants (including Blackberry or similar text messaging devices), pagers, telephones, cellular and mobile phones including those with cameras, intranet, Internet, back-up storage, information on a memory or flash key or card, jump or zip drive, any other type of internal or external removable storage drives or any other technology tool. In the remainder of this policy, all of these communication devices are collectively referred to as “Systems.”

## IV. PROCEDURES

### A. On-the-Job Use / Social Media

Department-Sanctioned Presence:

1. All department social media sites or pages shall be approved by the Chief of Police in accordance with City of Dunwoody policies.
2. Social media pages shall clearly indicate they are maintained by the department and shall have department contact information displayed.
3. Social media content shall adhere to applicable laws, regulations, and policies, including information technology and records management policies.
4. Content of social media pages is subject to Open Records laws.
5. Department personnel representing the department via social media outlets shall conduct themselves as representatives of the department and the City of Dunwoody and shall adhere to all department and City standards of conduct. They shall identify themselves as members of the department; not make comments regarding the guilt or innocence of suspects or arrestees; not make comments concerning pending prosecutions and not post, transmit or otherwise disseminate confidential information, including pictures, videos, evidence, or other materials in the department relating to training, work assignments, and enforcement efforts without the express written permission of the Chief of Police.
6. Department personnel shall not conduct political activities or private business on departmental social media.
7. The use of departmental computers, telephones, and other electronic communications devices to access social media is prohibited without the authorization of the Chief of Police.

8. Department personnel shall use personal electronic communications devices and computers to manage the department's social media sites only with the express written permission of the Chief of Police.
9. Department personnel shall observe and abide by all copyright, trademark, and service mark restrictions in posting materials to electronic media.

Social media is a valuable tool when seeking evidence or information regarding missing persons, wanted persons, gang activity, crimes perpetrated online, photographs or videos of a crime posted by a participant or observer.

10. Social media can be used for community outreach by providing crime prevention tips, offering online reporting opportunities, sharing crime maps and data, and soliciting tips about unsolved crimes.
11. Social media may be used for time-sensitive notifications of road closures, special events, weather emergencies, and missing or endangered persons.

## **B. Personal Use / Social Media**

Precautions and Prohibitions:

1. Department personnel are free to express themselves as private citizens on social media sites to the degree that their speech does not impair the work of the department for which confidentiality is important and does not impede the performance of duties.
2. Department personnel are cautioned that representing themselves as employees of the department in their off duty social networking may bring about targeting of the employee. The targeting of law enforcement personnel through social networking sites as a form of retaliation is documented.
3. Department personnel are cautioned that when using social media, their speech becomes part of worldwide electronic domain. Posting of personal photographs and other personal information by departmental personnel may subject them to becoming targets of criminal acts, harassment, or other forms of abuse due to their employment.
4. Department personnel shall adhere to the Code of Conduct when representing themselves as members of the department. They shall not post obscene or sexually explicit language, images, or acts and statements or other forms of speech that ridicule, malign, disparage, or otherwise express bias against any race, any religion, or any protected class of individuals.
5. Department personnel may not divulge information gained by reason of their authority; make statements, speeches, appearances, and endorsements; or publish materials that could reasonably be considered to represent the views or positions of this department without express authorization of the Chief of Police.

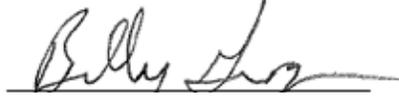
## **C. Agency and Personnel Electronic Devices**

Personal Computers, Cell Phones, and Recording Devices:

1. Department personnel and system users may not use personal laptops within any City building or leased space. Additionally, employees and system users may not use personal laptops to gain access to City network resources. Department personnel may have extenuating reasons for using a personal laptop, which must be approved by the Chief of Police.
2. Although incidental and occasional personal use of Systems that does not interfere or conflict with productivity or the City's business or violate City policy is permitted, personal communications in our Systems are treated the same as all other Electronic Communications and will be used, accessed, recorded, monitored, and disclosed by the City at any time without further notice. Since all Electronic Communications and Systems can be accessed without advance notice, employees and system users

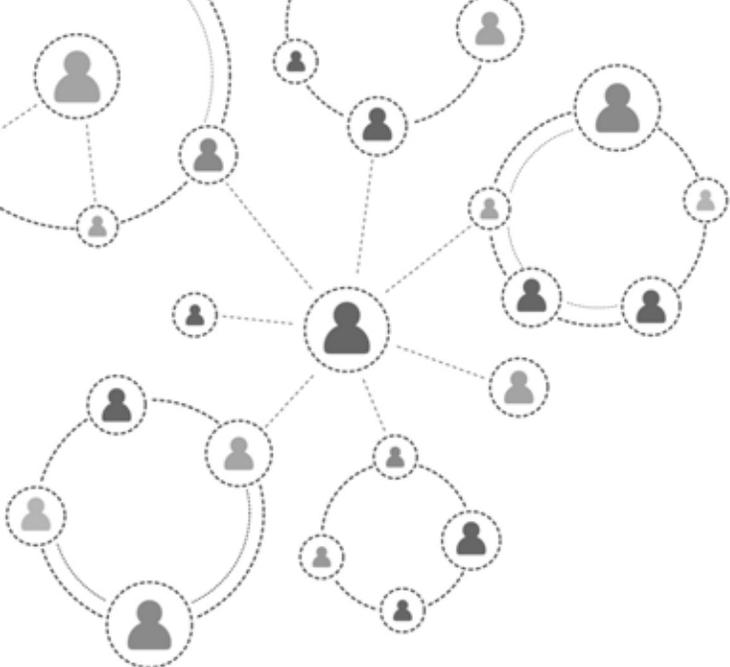
should not use our Systems for communication or information that they would not want revealed to third parties. Employees, therefore, shall not have any expectation of privacy regarding the use of our Systems.

3. The use of personal audio / visual recording devices while on duty and for the performance of assigned duties and responsibilities is prohibited unless otherwise authorized in writing by the Chief of Police.



Billy Grogan, Chief of Police  
Dunwoody Police Department

First Reading:	091111
Final Adoption	101311
Distribution Date	101411
Effective Date	111511



# APPENDIX D— NEW YORK CITY POLICE DEPARTMENT SOCIAL MEDIA POLICY

Data contained within social network sites may assist law enforcement in gathering timely information in furtherance of crime prevention, preservation of public order, and the investigation of criminal activity, including suspected terrorist activity. These guidelines are promulgated, in part, to instill the proper balance between the investigative potential of social network sites and privacy expectations.

Therefore, effective immediately, when a member of the service requires the use of social network websites to conduct investigations or research, the following procedure will be complied with:

## I. PURPOSE

To conduct social network-based investigations and research.

## II. SCOPE

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 members of the service to access social network sites using an online alias. No prior authorization is ever required for information contained on publicly available internet sources.

## III. DEFINITIONS

**Exigent Circumstances**—For the purpose of this procedure, circumstances requiring action before authorization can be obtained, in order to protect life or substantial property interest; to apprehend or identify a fleeing offender; to prevent the hiding, destruction or alteration of evidence; or to avoid other serious impairment or hindrance of an investigation.

**Online Alias**—An online identity encompassing identifiers, such as name and date of birth, differing from the user's actual name, date of birth, or other identifiers.

**Online Alias Access**—Internet-based searches involving the search and acquisition of information from sites that require an email address, password, or other identifiers for which an online alias is utilized.

**Public Domain Data**—Information accessible through the Internet for which no password, email address, or other identifier is necessary to acquire access to view or collect such information.

**Social Network Site**—Online platform where users can create profiles, share information, or socialize with others using a range of technologies.

<b>Procedure</b>	<b>When a member of the service requires access to a social network website for investigative or research purposes:</b>
<b>Member of the Service</b>	<ol style="list-style-type: none"><li>1. <b>Confer with supervisor, if access to public domain data requires the use of an online alias/online alias access.</b><ol style="list-style-type: none"><li>a. No conferral or authorization is required for general research, topical information or other general uses that do not require the acquisition of an online alias/online alias access.</li></ol></li></ol>
<b>Supervisor</b>	<p style="color: red;"><b>If application for online alias does not involve suspected terrorist activity:</b></p> <ol style="list-style-type: none"><li>2. <b>Evaluate request to determine whether an online alias would serve an investigative purpose, and if so, prepare Typed Letterhead requesting an online alias to bureau chief/ deputy commissioner concerned.</b></li><li>2. <b>Include on Typed Letterhead:</b><ol style="list-style-type: none"><li>a. Purpose for the request (i.e., type of investigation, etc.)</li><li>b. Tax registry number of requesting member</li><li>c. Username (online alias)</li><li>d. Identifiers and pedigree to be utilized for the online alias, such as email address, username and date of birth.</li><li>e. Do not include password(s) for online alias and ensure password(s) are secured at all times.</li><li>f. Indicate whether there is a need to requisition a Department laptop with aircard.</li></ol></li><li>4. <b>Review photograph to be used in conjunction with online alias, if applicable.</b><ol style="list-style-type: none"><li>a. Consider the purpose for which the photograph is being used and the source of the photograph.</li><li>b. Attach a copy of the approved photograph and indicate on Typed Letterhead how photograph was obtained.</li></ol></li></ol>
<b>Commanding Officer</b>	<ol style="list-style-type: none"><li>5. <b>Forward request to commanding officer for review.</b></li><li>6. <b>Review request(s) and consider the purpose and whether granting approval would serve an investigative purpose.</b></li><li>7. <b>Endorse request(s) indicating APPROVAL/DISAPPROVAL within one day of original request and if APPROVED, immediately forward approval to bureau chief/deputy commissioner concerned, through channels, for informational purposes.</b></li><li>8. <b>File copies of requests in command.</b></li></ol>

- Member of the Service 9. Maintain record of online alias in case records management systems or appropriate Department records.
- Bureau Chief/Deputy Commissioner 10. Maintain folder for each APPROVED online alias.
  - a. Designate an administrator for the online alias.

**If application for online alias involves suspected terrorist activity:**

- Supervisor 11. Immediately contact Intelligence Division, Operations Desk supervisor and provide details regarding proposed investigation.
- Intelligence Division, Operations Desk Supervisor 12. Determine if investigation should be conducted by the Intelligence Division and proceed accordingly.
- Supervisor 13. Notify requesting supervisor to proceed with investigation if it has been determined that the investigation will not be conducted by the Intelligence Division.
- Supervisor 14. Comply with steps “2” through “10”, as appropriate, if investigation will not be conducted by the Intelligence Division.

**When exigent circumstances exist that would warrant the immediate use of an online alias:**

- Supervisor 15. Confer with Intelligence Division, Operations Desk supervisor, if there is concern that the investigation may involve suspected terrorist activity.
  - a. Comply with instructions from Intelligence Division, Operations Desk supervisor.
- 16. Confer with commanding officer/executive officer, if investigation does not involve suspected terrorist activity.
- 17. Instruct member of the service to proceed with investigation upon receiving APPROVAL from commanding officer/executive officer.
  - a. Comply with steps “2” through “10”, as appropriate, and include in Typed Letterhead, the circumstances that led to the determination of exigent circumstances.

**Additional Data Legal Considerations**

During the course of an investigation, a member of service may need access to information regarding online accounts maintained by service providers. The federal Electronic Communications Privacy Act (ECPA) governs seizures of electronic evidence. Some information may be obtained with a subpoena; other information requires a special court order; and still other information requires a search warrant. Pertinent sections of the ECPA are as follows:

- a. A subpoena is generally deemed sufficient to obtain information such as user information and payment records.
- b. Electronic communications, such as email content, in electronic storage for 180 days or less may be obtained only after the issuance of a search warrant, and delayed notification to the subscriber or customer may be ordered if specifically requested in the search warrant application.
- c. Electronic communications in electronic storage for more than 180 days may be obtained with a subpoena signed by a judge; however, notice must be provided to the subscriber or customer unless the electronic communications are obtained after the issuance of a search warrant allowing for delayed notification.

**Additional Data  
(continued)**

- d. In anticipation of the issuance of a search warrant, a member of the service may send a request known as a “preservation letter” to an electronic service provider requesting the preservation of electronic records for 90 days, and extend the request for an additional 90 day period.

Note that particular service providers are known to ignore non-disclosure orders (i.e., some service providers will disclose the existence of a search warrant or subpoenas to a subject subscriber or customer.) In general, members of the service should consult with the Legal Bureau before seeking electronic communication through a search warrant or otherwise.

Data obtained through a grand jury subpoena or court order cannot be shared with other law enforcement agencies unless otherwise authorized.

**Operational Considerations**

When a member of the service accesses any social media site using a Department network connection, there is a risk that the Department can be identified as the user of the social media. Given this possibility of identification during an investigation, members of the service should be aware that Department issued laptops with aircards have been configured to avoid detection and are available from the Management Information Systems Division (MISD). A confidential Internet connection (e.g., Department laptop with aircard) will aid in maintaining confidentiality during an investigation. Members who require a laptop with aircard to complete the investigation shall contact MISD Help Desk, upon APPROVAL of investigation, and provide required information.

In addition to using a Department laptop with aircard, members of the service are urged to take the following precautionary measures:

- a. Avoid the use of a username or password that can be traced back to the member of the service or the Department;
- b. Exercise caution when clicking on links in tweets, posts, and online advertisements;
- c. Delete “spam” email without opening the email; and
- d. Never open attachments to email unless the sender is known to the member of the service.

Furthermore, recognizing the ease with which information can be gathered from minimal effort from an Internet search, the Department advises members against the use of personal, family, or other non-Department Internet accounts or ISP access for Department business. Such access creates the possibility that the member’s identity may be exposed to others through simple search and counter-surveillance techniques.

### **Department Policy**

The “Handschu Consent Decree” and “Guidelines for Investigations Involving Political Activity” (see Appendix “A” and “B” of Interim Order 58, series 2004, “Revision to Patrol Guide 212-72, ‘Guidelines for Uniformed Members of the Service Conducting Investigations of Unlawful Political Activities’”) require that any investigation, including investigations on social networks, by the New York City Police Department involving political activity shall be initiated by and conducted only under the supervision of the Intelligence Division. Accordingly, members of the service shall not conduct investigations on social networks involving political activity without the express written approval of the Deputy Commissioner, Intelligence. Any member of the service who is uncertain whether a particular investigation constitutes an “investigation involving political activity” shall consult with the Legal Bureau.

Members of the service who have created and used online aliases prior to the promulgation of this procedure must submit a request to continue utilizing the alias in accordance with this procedure.

#### **Related Procedures**

- Citywide Intelligence Reporting System (P.G. 212-12)
- Guidelines for Uniformed Members of the Service Conducting Investigations of Unlawful Political Activities (Interim Order 58, series 2004)

#### **Forms and Reports**

Typed Letterhead

Commanding officers will ensure that the contents of this Order are brought to the attention of members of their commands.

By Direction Of The Police Commissioner

Distribution

All Commands







### **About the Global Advisory Committee**

The Global Advisory Committee (GAC) serves as a Federal Advisory Committee to the U.S. Attorney General. Through recommendations to the Bureau of Justice Assistance (BJA), the GAC supports standards-based electronic information exchanges that provide justice and public safety communities with timely, accurate, complete, and accessible information, appropriately shared in a secure and trusted environment. GAC recommendations support the mission of the U.S. Department of Justice, initiatives sponsored by BJA, and related activities sponsored by BJA's Global Justice Information Sharing Initiative (Global). BJA engages GAC-member organizations and the constituents they serve through collaborative efforts, such as Global working groups, to help address critical justice information sharing issues for the benefit of practitioners in the field.