Law Enforcement and Technology: Using Social Media

January 11, 2022

Congressional Research Service
https://crsreports.congress.gov
R47008

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R47008

January 11, 2022

Kristin Finklea
Specialist in Domestic Security

Law Enforcement and Technology: Using Social Media

As the ways in which individuals interact continue to evolve, social media has had an increasing role in facilitating communication and the sharing of content online—including moderated and unmoderated, user-generated content. Over 70% of U.S. adults are estimated to have used social media in 2021. Law enforcement has also turned to social media to help in its operations. Broadly, law enforcement relies on social media as a tool for information sharing as well as for gathering information to assist in investigations.

Social Media as a Communications Tool. Social media is one of many tools law enforcement can use to connect with the community. They may use it, for instance, to push out bulletins on wanted persons and establish tip lines to crowdsource potential investigative leads. It provides degrees of speed and reach unmatched by many other forms of communication law enforcement can use to connect with the public. Officials and researchers have highlighted social media as a tool that, if used properly, can enhance community policing.

Social Media and Investigations. Social media is one tool in agencies' investigative toolkits to help establish investigative leads and assemble evidence on potential suspects. There are no federal laws that *specifically* govern law enforcement agencies' use of information obtained from social media sites, but their ability to obtain or use certain information may be influenced by social media companies' policies as well as law enforcement agencies' own social media policies and the rules of criminal procedure. When individuals post content on social media platforms without audience restrictions, anyone—including law enforcement—can access this content without court authorization. However, some information that individuals post on social media may be restricted—by user choice or platform policies—in the scope of audience that may access it. In the instances where law enforcement does not have public access to information, they may rely on a number of tools and techniques, such as informants or undercover operations, to gain access to it. Law enforcement may also require social media platforms to provide access to certain restricted information through a warrant, subpoena, or other court order.

Social Media and Intelligence Gathering. The use of social media to gather intelligence has generated particular interest from policymakers, analysts, and the public. Social media companies have weighed in on the issue of social media monitoring by law enforcement, and some platforms have modified their policies to expressly prohibit their user data from being used by law enforcement to monitor social media. Law enforcement agencies themselves have reportedly grappled with the extent to which they should gather and rely on information and intelligence gleaned from social media. For instance, some observers have suggested that agencies may be reluctant to regularly analyze public social media posts because that could be viewed as spying on the American public and could subsequently chill free speech protected under the First Amendment.

At the federal level, there is no specific legislative framework that governs law enforcement use of social media. Rather, there are laws and policies governing law enforcement investigations and intelligence gathering broadly. Some observers, however, have questioned whether the nature of social media may place it in a qualitatively different category than law enforcement's use of other investigative tools and have suggested that there should be enhanced boundaries with respect to law enforcement operations in these online spaces. For instance, some have suggested that law enforcement agencies should have written, publicly available policies on their use of social media; they should obtain local government approval before using these online spaces; they should obtain judicial approval for conducting undercover operations using social media; there should be restrictions on law enforcement contacting minors via social media; and law enforcement's use of social media should be audited. Policymakers may consider these issues as they conduct oversight or debate legislation on law enforcement use of social media.

Contents

Contacts

As the ways in which individuals interact continue to evolve, social media[1] has had an increasing role in facilitating communication and the sharing of content online—including moderated and unmoderated, user-generated content. Law enforcement has also turned to social media to help in its operations. Broadly, law enforcement relies on social media as a tool for information sharing as well as for gathering information to assist in investigations.

Over 70% of U.S. adults are estimated to have used social media in 2021, a substantial increase over the 5% of adults who were believed to use some form of social media in 2005.[2] Similarly, according to a 2016 survey of law enforcement agencies by the Urban Institute (Urban) and the International Association of Chiefs of Police (IACP) on their use of social media, it "is becoming an increasingly popular tool that law enforcement agencies use."[3] Law enforcement agencies use this tool for purposes including engaging with the public and gathering evidence pursuant to investigations. In the Urban and IACP survey, respondents indicated that they use social media for a variety of purposes, the most common being to notify the community of public safety concerns (91%). They also reported using social media for community outreach and citizen engagement (89%), public relations and notifying the community of non-crime issues (86%), soliciting crime tips (76%), monitoring public sentiment (72%), intelligence gathering for investigations (70%), and recruitment and applicant vetting (58%).[4] In addition, 60% of agency respondents indicated that they had reached out to a social media company to request information to use as evidence.[5]

There has been increased attention—particularly following high-profile incidents such as the January 6, 2021, attack on the U.S. Capitol[6]—on how law enforcement might access and use certain information shared on social media platforms to help prevent and investigate criminal activity. This report provides an overview of how law enforcement may leverage social media to communicate with the public and to aid in gathering information and evidence as part of its investigative duties. It also discusses information sharing between social media companies and law enforcement and raises issues that policymakers may consider as they examine the broader issue of how law enforcement may use social media.[7]

[1] For purposes of this report, social media is conceptualized as an internet-based platform that allows users to create individual and group profiles, generate content, and connect with other individuals and groups. These platforms include Facebook, YouTube, Instagram, Twitter, Pinterest, LinkedIn, Snapchat, WhatsApp, TikTok, Reddit, Nextdoor, and Parler among others. For more information on conceptualizing social media, see Jonathan Obar and Steve Wildman, "Social Media Definition and the Governance Challenge: An Introduction to the Special Issue," *Telecommunications Policy*, vol. 39, no. 9 (2015), pp. 745-750.

[2] Pew Research Center, *Social Media Fact Sheet*, April 7, 2021. The most widely used platforms are YouTube (81% of adults report having ever used) and Facebook (69%). Pew began its survey on this topic in 2005.

[3] Urban Institute and International Association of Chiefs of Police, *2016 Law Enforcement Use of Social Media Survey*, February 2017, p. 13.

[4] Ibid., p. 3. A total of 539 law enforcement agencies across the country participated in the survey.

[5] Ibid., pp. 4-5. An additional 9% indicated that they were uncertain whether or not their agency had reached out to a social media company to request evidence.

[6] Some planning of the incident reportedly occurred with the aid of social media. In addition, some participants and witnesses reportedly shared information on social media during and after the incident.

[7] For more information about social media, including issues involving misinformation and content moderation, see CRS Report R46662, *Social Media: Misinformation and Content Moderation Issues for Congress*.

Social Media as a Law Enforcement Communication Tool

Social media is one of many tools law enforcement can use to connect with the community. Law enforcement agencies, even without the use of social media, engage with the public to share and request information via newspaper, radio, television, and other media; push out bulletins on wanted persons; and establish tip lines to crowdsource potential investigative leads. However, social media provides degrees of speed and reach unmatched by many other forms of communication law enforcement uses to connect with the community.

Officials and researchers have highlighted social media as a tool that law enforcement agencies can use to improve public relations and enhance community policing.[8] For instance, the President's Task Force on 21st Century Policing—a Department of Justice (DOJ) task force established to identify best practices and offer recommendations on how law enforcement agencies can both promote crime reduction and build public trust—specifically cited technology and social media as tools that law enforcement agencies can leverage to build community engagement and trust.[9] The task force, in its 2015 report, noted that information shared on social media must be current and accurate so as not to harm trust and legitimacy.

Many observers have pointed to the Boston Police Department's use of Twitter during its evolving investigation of the Boston Marathon bombing in April 2013 as a social media use success story; reportedly, the Boston Police

> used Twitter to keep the public informed about the status of the investigation, to calm nerves and request assistance, to correct mistaken information reported by the press, and to ask for public restraint in the tweeting of information from police scanners. This demonstrated the level of trust and interaction that a department and a community can attain online.[10]

Federal law enforcement agencies have turned to a variety of social media platforms, including Facebook, Instagram, Twitter, YouTube, LinkedIn, and others to share information.[11] Some departments and agencies have designed policies specifically governing the use of social media to communicate with the public.[12]

---

[8] For more information on community policing, see CRS Report R43904, *Public Trust and Law Enforcement—A Discussion for Policymakers*. There are different conceptualizations of community policing, but there are common elements of what many argue may constitute it. These include emphasizing partnerships, promoting citizen input, focusing on prevention and problem solving, rethinking officer assignments and organizational structures, fostering positive interactions, and sharing information.

[9] President's Task Force on 21st Century Policing, *Final Report of the President's Task Force on 21st Century Policing*, May 2015.

[10] Ibid., p. 33. See also Edward F. Davis III, Alejandro A. Alves, and David Alan Sklansky, "Social Media and Police Leadership: Lessons from Boston," New Perspectives in Policing (Washington, DC: National Institute of Justice, March 2014).

[11] For a directory of social media accounts of the component agencies of the Department of Justice, see https://www.justice.gov/social.

[12] See, for example, Department of Justice, *DOJ Policy Statement: Use of Social Media to Communicate with the Public*, January 10, 2018. DOJ has also developed a Privacy Impact Assessment for its use of social media; see Department of Justice, *Adapted Privacy Impact Assessment for Use of Third-Party Social Media Tools to Communicate with the Public*, July 25, 2017.

Social Media and Investigations

Just as social media is one of many communication platforms used by law enforcement, it is also one tool among many others in agencies' investigative toolkits. There are a variety of means to help establish investigative leads and assemble evidence on potential suspects—including gathering information from social media sites. There are no federal laws that *specifically* govern law enforcement agencies' use of information obtained from social media sites, but their ability to obtain or use certain information may be influenced by social media companies' policies as well as law enforcement agencies' own social media policies and the rules of criminal procedure.[13]

The landscape of content available on social media platforms is broad, with users creating and sharing text, photos, and videos. Some platforms also have internal messaging services where users can communicate directly with other users of the platform.[14] Access to this social media content is influenced by factors including social media platform policies and user controls. Some content is available to a broad audience without restriction; other content contains access boundaries. Individuals generally have some control over the intended audience with whom they share content. Facebook users, for instance, can elect to share content publicly, with only Facebook contacts/friends (or some subset of friends), with Facebook friends and their friends, with a specific Facebook group, or may post information privately that no one else sees. And, depending on settings, consumers of social media content may be able to, in turn, share or re-share a friend's/contact's content, thus potentially expanding the audience of this content beyond what may have been initially intended by the individual who created or first shared it.

Accessing Public Information

When individuals post content on social media platforms without audience restrictions, anyone who visits the platforms—including law enforcement—can access this content. Law enforcement does not need to obtain court authorization to view content that has been published for any and all to see, like a sign in one's yard.[15]

In addition to content that one shares on social media, selected account-level information may also be available to a broad audience, including law enforcement, such as the information contained in a public profile. Depending on platform and user settings, this may include a host of demographic, geolocation, and other data, potentially including a list of other accounts with whom one is connected on a given social media platform. Law enforcement may use this information to learn more about an individual's social network.

[13] For instance, DOJ's *Justice Manual* has guidelines on personal use of social media (see Section 1-9.000, https://www.justice.gov/jm/jm-1-9000-personal-use-of-social-media) and on evidence collection, including searches and seizures (see Section 1-13.000, https://www.justice.gov/jm/jm-9-13000-obtaining-evidence). Federal law enforcement agencies are also subject to the Federal Rules of Criminal Procedure. For more information, see CRS In Focus IF11557, *Congress, the Judiciary, and Civil and Criminal Procedure*.

[14] Access to these communications may be affected by social media policies, law enforcement rules for criminal procedure, and whether or not the communications are encrypted.

[15] In 1999, DOJ convened an Online Investigations Working Group with representatives from across DOJ as well as members from the Department of the Treasury, Department of Defense, and others. A copy of the working group's November 1999 report, *Online Investigative Principles for Federal Law Enforcement Agents*, is available at https://info.publicintelligence.net/DoJ-OnlineInvestigations.pdf. It detailed a range of principles for online investigations. These principles may apply to investigations involving social media, though it is unclear to what extent federal law enforcement may rely on such principles today.

Although law enforcement may be legally and technically able to access public information on social media platforms, agencies may have internal policies governing this access. These internal policies may, for instance, place restrictions on the circumstances under which law enforcement can access social media for investigations as well as the authorization needed to do so.[16]

Accessing Restricted or Private Information

Based on platform policies or user choices, some information that individuals post on social media may contain restrictions regarding the breadth of the audience that may access that information. Some of these restrictions are established by platform controls and some may be established by user preferences. In the instances when law enforcement does not have public access to information, they may rely on a number of tools and techniques to gain access to it.

For instance, law enforcement may rely on informants, or contacts of the persons about whom law enforcement is seeking information, to share social media information that they may have access to because of their status as a direct contact with the individual in question. Law enforcement may also operate undercover, posing as someone who may be more likely to gain access to an individual's social media network in order to glean information.[17] Some observers have suggested that law enforcement agencies should specifically address the use of online aliases in their social media policies to draw a distinction between the information they gather that is unrestricted and publicly available and that which they gather through the use of an alias.[18]

Law enforcement may also require social media platforms to provide access to certain restricted information through a warrant, subpoena, or other court order. For instance, law enforcement may want to access private information from a particular individual's account pursuant to an investigation and may need a warrant to do so. Similarly, as some social media posts or comments on public forums are made anonymously, law enforcement would generally need a warrant to try and obtain information from the platform on the identity of the anonymous poster.

Preservation Request

In some instances, law enforcement may present social media companies with a request to preserve certain content at a particular moment in time. This may be done to prevent content from being altered during the time it takes law enforcement to obtain the proper court authorization, such as a warrant, needed to obtain access to this content. Wire and electronic service providers as well as remote computing services, including social media platforms, are required to preserve content for 90 days at the request of law enforcement. This request may be extended once for an additional 90-day period.[19] Following the January 6, 2021, attack against the U.S. Capitol,

[16] For instance, the Honolulu Police Department requires that officers obtain approval from the Chief of Police or a designee before using social media to conduct an investigation. See Honolulu Police Department, Policy, Organization, Management, and Administration, *Policy Number 2.72: Social Media*, May 21, 2019. Studies have recommended that law enforcement develop social media policies (see, for instance, Bureau of Justice Assistance with the Global Justice Information Sharing Initiative and Criminal Intelligence Coordinating Council, *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations*, February 2013). It is unclear how many agencies have these policies or whether the policies may be publicly available. The Brennan Center for Justice has collected some publicly available social media policies and collated them online at https://www.brennancenter.org/our-work/research-reports/directory-police-department-social-media-policies.

[17] For instance, DOJ has guidelines for FBI undercover operations. These guidelines reference undercover operations online, but they do not have specific guidance on operations involving social media. See Department of Justice, *The Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations*, May 30, 2002.

[18] U.S. Department of Justice, Community Oriented Policing Services and Police Executive Research Forum, *Social Media and Tactical Considerations for Law Enforcement*, July 2013.

[19] 18 U.S.C. §2703(f).

there was concern that participants in the attack and others may attempt to edit or remove content that they had posted, shared, or otherwise engaged with leading up to and following the attack. As such, reporting indicates, federal investigators requested that companies such as Facebook, Twitter, and others preserve this content that could help in their investigations.[20]

Platform Policies on Information Sharing with Law Enforcement

Pursuant to the Stored Communications Act (Title II of P.L. 99-508), social media platforms may disclose information about users and their communications on the platform to law enforcement under certain circumstances. For instance, platforms may disclose certain information to law enforcement with a warrant or other valid court order. Platforms may also share information with law enforcement if they, in good faith, believe that there is an emergency involving a danger of death or serious injury.[21] Social media platforms also have a lawful duty to report apparent or imminent violations of federal law pertaining to child sexual exploitation and child sexual abuse material.[22]

Sharing Information on Child Sexual Abuse Material

Violations of federal law with respect to child sexual exploitation and child sexual abuse material (CSAM) are the one area of malicious behavior on which electronic service providers—including social media platforms—must report if they have knowledge of its occurrence. The duty to report applies in instances of apparent or imminent violations of 18 U.S.C. §§2251, 2251A, 2252, 2252A, 2252B, or 2260 that involve child pornography, or what is commonly referred to as CSAM. Specifically, providers must report to the CyberTipline, which is operated by the National Center for Missing and Exploited Children (NCMEC).[23] NCMEC makes these reports available to law enforcement investigating crimes relating to child sexual exploitation.

The duty to report apparent or imminent child sexual exploitation does not also place a duty on providers to actively search for this content. Rather, the duty to report only applies to content that a provider becomes aware of. Nonetheless, some social media platforms such as Facebook have started to take steps toward proactively detecting this content in their systems.[24]

Policymakers have debated whether this model, of requiring electronic service providers to report apparent or imminent violations related to child sexual exploitation, can or should be replicated for other forms of malicious behavior occurring online, with a specific focus on social media platforms.

In addition to what is allowable or required by law, social media platforms establish internal policies, which may vary from platform to platform and may change over time, regarding information sharing with law enforcement.[25] They may voluntarily share information with law enforcement that is not protected by, or in violation of, the privacy agreements they have established with their users. There is also the issue of whether social media companies are

[20] Brooke Singman, "Big Tech 'complying' with federal requests to preserve evidence on social media amid Capitol riot probe," *Fox News*, January 28, 2021.

[21] 18 U.S.C. §2702.

[22] 18 U.S.C. §2258A. This statute makes it a duty to report for all electronic service providers, which includes social media platforms.

[23] NCMEC is a resource center for law enforcement agencies working on cases of missing and exploited children. NCMEC personnel take reports of missing and exploited children through a hotline and online portal, the CyberTipline.

[24] Agnus Crawford, "Whistleblower: Facebook's response to child abuse 'inadequate'," *BBC News*, October 28, 2021. See also Facebook's policies on child safety at https://www.facebook.com/safety/onlinechildprotection.

[25] For instance, Facebook and Instagram policies on information sharing with law enforcement are outlined at https://www.facebook.com/safety/groups/law/guidelines/. Twitter's guidelines for law enforcement are available at https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support.

disincentivized to proactively search for certain malicious content on their platforms if they are shielded from liability for content hosted on their platforms.[26]

Even if social media companies want to share certain information with law enforcement, they may not be able to do so if the information is encrypted in such a way that the company cannot access it. For instance, WhatsApp Messenger implemented default end-to-end encryption on its platform in 2016. This form of strong encryption, what some have termed *warrant proof* encryption, prevents WhatsApp from accessing the content of communications, even if presented with a warrant, because it does not hold the key to unlock the encrypted communications.[27] Meta, the parent company of WhatsApp, Facebook, and Instagram, announced that it would implement end-to-end encryption on Facebook's and Instagram's Messenger service; however, this encryption shift is reportedly delayed until at least 2023.[28]

Intelligence Gathering via Social Media

In addition to using social media to help communicate with the public and further investigations, law enforcement agencies also rely on it for intelligence gathering purposes. This is the use that arguably has generated the most questions from policymakers, analysts, and the public. There have been questions about the extent to which law enforcement is actually using social media for intelligence gathering, how they might store and use such information, whether this intelligence gathering can hinder First Amendment protected activities, whether social media monitoring may undermine privacy rights, and whether intelligence gathering disproportionally affects certain individuals or communities.[29]

Social media companies have at times weighed in on the issue of social media monitoring by law enforcement. These companies provide access to their user data to developers that build tools to improve user experiences, conduct research, and monitor social media platforms, among other things.[30] Following reports that some law enforcement agencies had been monitoring social media with developers' tools built on platforms' user data, some platforms changed their policies to expressly prohibit their user data from being used by law enforcement to monitor social media.[31]

In addition, law enforcement agencies themselves have reportedly grappled with the extent to which they should gather and rely on information and intelligence gleaned from social media. For instance, some observers have suggested that agencies such as the Federal Bureau of Investigation (FBI) may be reluctant to regularly analyze public social media posts because that

[26] Section 230 of the Communications Decency Act of 1996 (CDA) is generally seen as protecting social media sites from liability for hosting content. A discussion of the current debate surrounding Section 230 is outside the scope of this report; however, for more information, see CRS Report R45650, *Free Speech and the Regulation of Social Media Content*.

[27] For more information on *warrant-proof* encryption and the tension between law enforcement and technology companies, see CRS In Focus IF11769, *Law Enforcement and Technology: the "Lawful Access" Debate*.

[28] Dan Milmo, "Meta delays encrypted messages on Facebook and Instagram to 2023," *The Guardian*, November 21, 2021.

[29] See, for instance, Brennan Center for Justice et al., *Civil Rights Concerns about Social Media Monitoring by Law Enforcement*, November 6, 2019.

[30] Twitter Developer Platform, *Tap Into What's Happening to Build What's Next*, https://developer.twitter.com/en.

[31] Brennan Center for Justice, *Map: Social Media Monitoring by Police Departments, Cities, and Counties*, July 10, 2019. See also Chris Moody, Twitter Developer Platform Blog, *Developer Policies to Protect People's Voices on Twitter*, November 22, 2016.

could be viewed as spying on the American public and could subsequently chill free speech.[32] Others, however, have noted that the benefits to national security and public safety from analyzing social media content outweigh the risks.[33] The Attorney General's Guidelines for Domestic FBI Operations (Guidelines) specifically note that online services and resources may be used in intelligence assessments that may help detect and interrupt criminal activities at their early stages. The Guidelines state that

> assessment activities may proactively involve surfing the Internet to find publicly accessible websites and services through which recruitment by terrorist organizations and promotion of terrorist crimes is openly taking place; through which child pornography is advertised and traded; through which efforts are made by sexual predators to lure children for purposes of sexual abuse; or through which fraudulent schemes are perpetrated against the public.[34]

There are numerous instances of law enforcement relying on social media in support of intelligence assessments and investigations. For instance, following the May 2020 killing of George Floyd, there were numerous protests around the country, and FBI agents "monitored social media activity for imminent acts of violence."[35] The FBI has contracted with various social media monitoring companies to "obtain early alerts on ongoing national security and public safety-related events through lawfully collected/acquired social media data."[36] In addition, DHS is reportedly considering enhancing its existing intelligence efforts to examine information from social media to better understand potential security threats and identify likely targets.[37] To do so, DHS may leverage the expertise of private companies to help analyze publicly available content posted on social media. This reevaluation of DHS's capabilities in social media analysis comes on the heels of the January 6, 2021, U.S. Capitol attack; DHS intelligence reportedly did not detect and/or report the security threats that were discussed on social media.[38]

In another example, the mayor of Chicago announced in August 2020 that the Chicago Police Department created a specialized social media task force to monitor online activity with the goal of preventing looting. The 20-person unit was tasked with collecting intelligence, including through the use of data analytics and searching social media pages and accounts that had been associated with organizing looting activity. The task force was also reportedly working with other law enforcement partners, including the FBI, to investigate looting incidents that had already occurred.[39]

[32] Ken Dilanian, "DHS Launches Warning System to Find Domestic Terrorism Threats on Public Social Media," *NBC News*, May 10, 2021.

[33] Ibid.

[34] Department of Justice, *The Attorney General's Guidelines for Domestic FBI Operations*, September 29, 2008.

[35] Affidavit in Support of Criminal Complaint, United States v. Avery, 4:20-mj-07180, May 31, 2020.

[36] Federal Bureau of Investigation, Finance Division, Procurement Section, *Request for Proposals (RFP) No. / 15F06720R0000063*, January 28, 2020. The FBI has had agreements with companies such as DataMinr and ZeroFox; see Ken Dilanian, "Why did the FBI miss the threats about Jan. 6 on social media?", *NBC News*, March 8, 2021.

[37] Rachael Levy, "U.S. Social Media Push Would Use Outside Monitors," *Wall Street Journal*, August 16, 2021.

[38] Ibid. See also Ken Dilanian, "DHS Launches Warning System to Find Domestic Terrorism Threats on Public Social Media," *NBC News*, May 10, 2021.

[39] "Chicago Authorities to Monitor Social Media Amid Looting Threats, Lightfoot Says," *NBC Chicago*, August 14, 2020.

Going Forward

There is no specific federal legislative framework that governs law enforcement use of social media.[40] Rather, there are laws and policies governing law enforcement investigations and intelligence gathering, broadly. Some observers, however, have questioned whether the nature of social media may place it in a qualitatively different category than law enforcement's use of other investigative tools and have suggested that there should be enhanced boundaries with respect to law enforcement operations in these online spaces. For instance, some have suggested that law enforcement agencies should have written, publicly available policies on their use of social media; they should obtain local government approval before using these online spaces; they should obtain judicial approval for conducting undercover operations using social media; there should be restrictions on law enforcement contacting minors via social media; and law enforcement's use of social media should be audited.[41] Policymakers may consider these issues as they conduct oversight or debate legislation on law enforcement use of social media.

Oversight of Law Enforcement Social Media Policies

The President's Task Force on 21st Century Policing, as well as various DOJ research partnerships,[42] have recommended that law enforcement agencies develop policies governing the use of social media. For instance, the Bureau of Justice Assistance (BJA) sponsored a project in collaboration with the Global Justice Information Sharing Initiative[43] that, in 2013, recommended "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."[44] Specifically, it recommended that a social media policy should accomplish the following:

- note that use of social media will be in accordance with relevant laws, regulations, and agency policies;
- define if and when use of social media sites/tools is permitted;

[40] In addition, there is not yet a wide body of case law to help inform on how courts are viewing law enforcement's use of social media.

[41] See, for example, Rachel Levinson-Waldman and Angel Diaz, *How to Reform Police Monitoring of Social Media*, Brookings, July 9, 2020.

[42] Emily Tiry, Ashlin Oglesby-Neal, and KiDeuk Kim, *Social Media Guidebook for Law Enforcement*, Urban Institute, February 2019. See also Edward F. Davis III, Alejandro A. Alves, and David Alan Sklansky, "Social Media and Police Leadership: Lessons From Boston," *Harvard Kennedy School and National Institute of Justice: New Perspectives in Policing*, March 2014; and Bureau of Justice Assistance with the Global Justice Information Sharing Initiative and Criminal Intelligence Coordinating Council, *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations*, February 2013.

[43] 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).

[44] Bureau of Justice Assistance with the Global Justice Information Sharing Initiative and Criminal Intelligence Coordinating Council, *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations*, February 2013, p. 6.

- specify the authority needed to use information obtained from social media;
- note that information acquired from social media will be evaluated to assess reliability and validity;
- specify documentation, storage, and retention requirements surrounding information obtained from social media;
- define any guidelines involving off-duty personnel using social media information in connection with official duties and when/how personal equipment may be used for an authorized law enforcement purpose; and
- identify procedures for disseminating criminal intelligence and investigative products that contain information obtained from social media, including any parameters for disseminating personal information.

Anecdotal reports of law enforcement officers being reprimanded for improper use of social media have highlighted the sensitive nature of law enforcement personnel using social media in their personal and professional capacities.[45] Policymakers may seek to evaluate whether federal law enforcement agencies have social media policies in place as well as how the agencies conduct oversight of officers' use of social media.

Congress can legislate directly on federal law enforcement practices, and it can also influence state, local, and tribal policies and practices through the provision or withholding of grant funding. Programs such as the Edward Byrne Memorial Justice Assistance Grant (JAG) program[46] and the Community Oriented Policing Services (COPS) program[47] have been used to incentivize activities of state and local law enforcement and may be leveraged to influence the adoption of social media policies. The federal government can also affect state, local, and tribal policies through the transfer of knowledge and expertise. For instance, BJA and its partners have provided guidance and recommendations on developing a social media policy that law enforcement agencies may reference.[48]

Data on Frequency of Social Media Use in Investigations and Intelligence Gathering

Although there have been some surveys of law enforcement on how they use social media and for which purposes, data are lacking on the extent to which law enforcement agencies leverage public information on social media platforms as well as restricted information gleaned through lawful means such as warrants and subpoenas. Some observers report that law enforcement has increasingly turned to social media content to assist in their investigations, while others have suggested that some law enforcement agencies are shying away from analyzing public social media posts because it may be viewed as spying on the public.[49]

[45] See, for example, Donald J. Mihalek and Richard M. Frankel, "The dangers of social media for law enforcement take center stage amid series of scandals: Analysis," *NBC News*, July 11, 2019.

[46] For more information, see CRS In Focus IF10691, *The Edward Byrne Memorial Justice Assistance Grant (JAG) Program*.

[47] For more information, see CRS In Focus IF10922, *Community Oriented Policing Services (COPS) Program*.

[48] Bureau of Justice Assistance with the Global Justice Information Sharing Initiative and Criminal Intelligence Coordinating Council, *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations*, February 2013.

[49] Ken Dilanian, "DHS Launches Warning System to Find Domestic Terrorism Threats on Public Social Media," *NBC News*, May 10, 2021.

Congress may consider tasking oversight entities such as the Government Accountability Office or department-level Inspectors General with reporting on issues such as whether law enforcement agencies have established clear parameters on the use of social media for investigations and intelligence gathering, whether or how agencies note the use of social media in investigative case files, and whether or how agencies tabulate metrics on their use of social media or other related tools. Congress may also request such information from law enforcement agencies directly through letters, hearings, and other oversight. A greater understanding of the purposes for and extent to which law enforcement relies on social media in its investigations and intelligence gathering may provide a stronger foundation for policy discussions going forward.

Author Information

Kristin Finklea
Specialist in Domestic Security

Disclaimer