THE USE OF SOCIAL MEDIA AS A SUPERVISION TOOL

American Probation and Parole Association

Submitted by the Technology Committee

April 24, 2019

ISSUE PAPER

THE USE OF SOCIAL MEDIA AS A SUPERVISION TOOL

INTRODUCTION

Social media platforms allow users to engage with each other using the Internet to participate in, comment on, and create content, including photos and videos, as a means of communication. Examples of social media include blogs, social networking sites (such as Facebook, Twitter, LinkedIn, Pinterest, Google+, Tumblr and Instagram), and other location-based networks. Social media use has grown rapidly. Indeed, social media usage among American adults has increased from 5% in 2005 to 69% today (Pew Research Center, 2018), with, not surprisingly, 88% usage by young adults aged 18 to 29, the demographic most likely to use social media (Pew Research Center, 2018).

The advent of social media has made it much easier for individuals to find and interact online with others who share similar interests. All this drives discovery, sharing, activism, and influence. Given the prevalence of social media in contemporary society, it is imperative that community corrections agencies take note and explore opportunities to leverage this phenomenon in a way that supports their mission. For example, by monitoring social media activity, agencies can review client[1] posts, identify a client's friends and associates, locate those who have absconded, observe violations in real time, and generally keep better track of those under their supervision. While social media monitoring can yield important information, this is a relatively new area with little guidance to help agencies understand the corresponding ethical and operational issues.

1 The term client will be used in this paper to refer to adults and juveniles involved with community corrections agencies as pretrial or presentence defendants or persons under probation, parole, or other forms of community supervision.

This paper will present an overview of the issues agencies should consider as they determine whether and how to leverage this strategy as part of the investigation and supervision process. Specifically, this paper addresses the potential justifications for monitoring client social media activity, specific implementation issues to be examined and addressed, and the need to establish sound policies to guide officers in the proper use of these tools.

HOW SOCIAL MEDIA MONITORING FITS INTO A COMMUNITY SUPERVISION MISSION

To be most effective, community supervision officers should gather and process relevant information about the individuals under their charge. This knowledge may be initially sought prior to conviction and sentencing, in the pretrial and presentence investigation stages (Clear & Cole, 1990). Later, as part of the supervision process, officers must monitor compliance with the conditions of probation or parole and client progress towards their goals. Historically, investigations and intelligence were conducted by interviewing clients and their collateral contacts, carrying out home and field visits, and reviewing paper reports/records. However, given that the majority of the population, which includes justice-involved individuals, now has a social media presence, agencies should consider expanding their purview beyond the brick and mortar world to include the virtual realm.

To be most effective, community supervision officers should gather and process relevant information about the individuals under their charge.

One of the most compelling reasons for reviewing a client's social media activity can be termed the "window into their mind" effect (Tanner, 2007). Individuals, particularly teens and young adults, have a tendency to post information, including photos, online that is not otherwise normally disclosed to others (Buzzetto-More, Johnson, & Elobaid, 2015). This information is frequently posted in public areas, viewable by anyone. By accessing social networking sites, officers may find important information that otherwise might not be readily available to them.

With these opportunities come challenges that agencies will need to consider and address to ensure officers understand how to use social media monitoring in an ethical manner, consistent with an agency's mission and values. The following section will discuss some of these challenges.

JUSTIFICATIONS FOR SOCIAL MEDIA MONITORING

Agencies should be able to articulate a clear justification for examining social media activity beyond merely stating that it is part of a client's supervision. Further, not every client's social media activity needs to be scrutinized equally. Agencies should determine how to use this tool on an individual, case-by-case basis that considers factors such as risk level and offense type. Some examples of justifications include:

Pre-Trial/Pre-Sentence Investigation and Report Preparation

Agencies regularly develop investigative reports to provide a court with background on clients to assist in making critical decisions such as pretrial release, sentencing, and juvenile court dispositions. A constant concern about these reports is the extent to which they accurately portray the person before the court. Examples of issues that may be unclear or difficult to establish definitively include whether the person is truly remorseful for conduct, whether the person is being honest about a substance abuse problem or a gang association, and whether the person has disclosed complete and accurate information about all assets (Bowker, 1998). As part of the investigation process, an examination of a client's social media activity may reveal information that either contradicts or supports the image the convicted person is trying to convey to the judge.

General Supervision

Reviewing social media activity can provide important insight into behaviors that can be indicative of a client's progress. Below are some common examples of behaviors discovered while monitoring social networking sites.

Criminal behavior: Clients may post threats against significant others, informants, witnesses, judges, individual officers, and/or agencies in general (Gokavi & Stewart, 2018). Clients may use social media sites as a vehicle to continue their criminal operations (e.g., selling drugs). In some cases, clients do not try to hide their activities but instead freely post pictures or videos of themselves posing with firearms or bragging about a criminal act, such as a robbery recently committed (Baldas, 2015; CBS, 2018). These activities may be part of a relatively new phenomenon termed "performance crime," which is an illegal act committed with the intention of being witnessed by an audience or seeking an audience after the fact (Surette, 2015).

A constant concern about these reports is the extent to which they accurately portray the person before the court.

Sex offender management: Supervision conditions or statutes prohibit sex offenders from accessing social networking sites. In some cases, clients may be restricted from the Internet entirely. In these instances, an officer can search for such a client's profile and investigate possible matches to determine whether a violation has occurred. In cases where these clients are allowed access to social media, it may be critically important that officers monitor their online activities as part of the containment model (Pimentel & Muller, 2010).

Criminal/gang associations: Standard supervision conditions preclude clients from associating with co-defendants, convicted felons, or other persons deemed inappropriate (Clear & Cole, 1990). Checking social media activity can provide information as to the client's compliance with these directives. Gang members are frequently observed associating with one another online, freely displaying gang signs or colors (Korn, 2015).

Substance abuse: Clients will sometimes reference their drug or alcohol use in social media posts (Jones, 2014; Sweeney, 2012). Further, these posts may establish association with other known abusers. Some clients may use social media to investigate methods to defeat drug or alcohol testing. Officers who become aware of these behaviors are better positioned to confront their clients and develop an appropriate response, whether it be additional testing, treatment, or a sanction.

Unauthorized leave: Some clients will post images of themselves traveling outside of a jurisdiction without permission (Bologna, 2018). Those with home confinement restrictions may post updates reflecting that they are not at an authorized location, such as work. Clients may not realize that the devices they use to upload content onto social networking sites also can add geolocation data to the post (Murphy, 2010). This information, if available, can be very important, particularly if the context of the image leaves some doubt about actual location (e.g., was a picture of the Eiffel Tower taken in Las Vegas or Paris?). The geolocation data embedded in a post or image removes this doubt.

Other non-compliance: Social media activity often displays other behaviors of concern that officers may wish to investigate further. For example, clients may post photos of themselves with unexplained assets, such as the display of large amounts of cash (Eiseman, 2010), or "goofing-off" at work and potentially jeopardizing their employment situation.

Fugitive Apprehension

Social networking sites have been extremely helpful for locating absconders from supervision (Bernstein, 2012; Rayborn, 2009). Absconders often remain active on social media even while seeking to elude authorities. The contacts, status updates, and pictures they post (and associated geolocation data) are invaluable clues to apprehension. Further, several community corrections agencies have established their own social media sites specifically to inform the public and enlist their support in locating absconders (Mississippi Department of Corrections, 2018). These sites typically display client photos, their offenses, and the contact information to report wanted persons.

Officer Safety

Information gleaned from a client's social media activity can be vital to an officer's personal safety. For example, clients may post information about the weapons they can access, drug use, training in hand-to-hand combat, presence of dangerous animals in the home, or violent associates (Haddad, 2018). As mentioned earlier, some

clients may post direct threats against officers (Grimes, 2015). Further, social networking sites such as Twitter may give officers insight into the general "climate" of a neighborhood they are about to enter. For example, it may be important to know there is rising anti-law enforcement sentiment or that there may be protests or unrest in response to a recent incident (Peet, 2012). Some larger agencies may consider using social media aggregator tools, such as Media Sonar and DataMinr, which gather data and disseminate information on trends in an area (Freger, 2018).

IMPLEMENTATION CONSIDERATIONS AND MONITORING APPROACHES FOR SOCIAL MEDIAL MONITORING

Clearly, there are numerous rationales for monitoring client social media activity. The following section will outline the implementation issues that agencies will have to consider and address before incorporating this technique into their operations.

Officers can use a variety of methods to search for and monitor a client's social media activity. A policy guide on the use of social media in intelligence and investigative activities developed by the Global Justice Information Sharing Initiative Advisory Committee (Global) notes three distinct methods: *Apparent/Overt Use, Discrete Use,* and *Covert Use* (Global, 2013). Each approach has a different level of intrusiveness.

Apparent/Overt Use

Apparent/Overt Use involves accessing of social networking sites without any interaction with the targeted individual (Global, 2013). The access is limited to information in the open or "public" areas of social media sites. For instance, depending on the user's privacy settings on any given social media site, an officer could view a client's entire profile, friends, photos, videos, and/or posts. However, access would not include information contained in the client's social networking site email messages or to data behind a restricted area set by the client.

Discrete Use

Discrete use involves techniques concealing the officer's identity, but no direct online interaction with the client occurs (Global, 2013). It differs from Apparent/Overt use in that anonymous tools, such as proxy servers or websites or a fictitious identity, are used. Some techniques, such as using an anonymizing proxy server or website, which strips the officer's originating Internet Protocol (IP) address from all communications between him/her and a target website, may be used to obscure the fact that these communications are coming from an officer/agency. In some cases, a fictitious identity is created to allow the user to access public areas of social networking sites without disclosing who they are to other members of the site.

Covert Use

The most intrusive method is covert use, and this requires special training and equipment and specific authorization (Global, 2013). This method involves concealing the officer's identity and then directly engaging with the client to gain information and/or evidence of a violation that may take place. A fictitious identity should not use a real person's name or image, as there can be serious repercussions for the real person if something goes amiss during the investigation, creating a civil liability for the agency. The safest option may be to use the social media provider's generic silhouette icon in place of a photo. When using this approach, the agency must take care not to entrap the offender, i.e., induce the individual to commit a crime he or she was not predisposed to commit (Shipley & Bowker, 2014). Further, agencies must recognize that creating a fictitious profile may violate the site's terms of service. While many law enforcement agencies routinely ignore these terms, the practice remains unauthorized and, if discovered, the site will delete the profile without advance notice to the creator (Maas, 2018).

Review with Client Cooperation

One additional investigative method is the ability to require clients to provide access to their profiles (Bowker, 2011). Officers must be diligent in obtaining written disclosure on all social media profiles used by a client, including all email accounts, and this information should be updated regularly. If clients are not forthcoming about profiles, officers may investigate third party contacts, conduct computer or Internet searches, or inquire with various paid data brokers. In higher-risk cases or those involving sexual offenses, polygraph testing may be leveraged (Bowker, 2012).

Once a client's profile has been identified, officers can request their client to allow them to briefly connect to the profile with the use of an investigative profile. This allows the officer to remotely review the client's contacts, posts, and/or photos on social networking sites from their investigative profile. This is the least intrusive method of conducting a review. However, it will not provide the officer access to the client's email and/or chat messages or to their client's restricted areas.

Another variation is to require clients to access their social media profile in the officer's presence for a review, which would provide access to information in the public locations along with additional information that they have chosen to keep private, even from their connections. This method does not require the officer to have a profile; however, it is more intrusive than the first option. Further, officer safety may be a concern due to the potential immediate revelation of violations or criminal acts. Some social media sites permit the download of the entire user's activity, which can be reviewed later by the supervision officer (Matsakis, 2018).

INFRASTRUCTURE AND SECURITY

Social media monitoring raises a variety of information technology infrastructure and security issues that agencies will need to address. For example, officers will need access to the Internet to perform this function. This may seem obvious. However, not every agency allows this, due to network security concerns (Russo & Matz, 2014). Some officers may want to use their personal devices and accounts to gain access, but this practice should be discouraged. The device used to monitor a client's social media activity may be collected as evidence, which creates the risk of exposing the officer's sensitive personal information in court. Agencies providing their officers access to the Internet should consider measures to protect the integrity of their information systems, as the use of unsecure computers can introduce malware that can compromise not only the investigation but also the agency's main network (Shipley & Bowker, 2014).

To mitigate these risks agencies should designate computers specifically for this purpose, isolate them from the agency's network, and provide separate Internet access, such as Wi-Fi. Such a configuration avoids exposing the agency's entire IT systems to potential harm while also eliminating any risk to an employee's personal computer and information. Unfortunately, separate access does not automatically translate into security. A firewall must be used and kept current. Designated computer software, including anti-virus and anti-spyware applications, must be maintained and kept updated. To ensure that the designated computer is used only for work-related purposes, controls need to be established, such as separate user accounts and installation of monitoring software (Shipley & Bowker, 2014).

AUTHENTICATION OF INFORMATION

Shipley & Bowker (2014) refer to anything posted on social networking sites as "online electronically stored information" (OESI). Agencies should consider the implications of using OESI, with specific attention to the need for authentication, which has two components. Information stored online is easily altered or deleted. Authentication requires that officers collect and preserve OESI in a manner establishing that what they collected is what they actually saw online and was not altered after collection. This establishes a chain of custody for OESI that will be needed for use in any legal proceeding (Shipley & Bowker, 2014).

The second component of authentication requires officers to gather corroborating or supporting evidence that the OESI they collected is what it purports to be, as this is not always clear. For example, obtaining an admission or confession from the offender, interviewing witnesses, obtaining information from the respective Internet Service Provider, and collecting digital evidence from the pertinent devices can help provide proper authentication (Shipley & Bowker, 2014).

POTENTIAL FOR LIABILITY

As with any other initiative, agencies should carefully consider their vulnerability to liability. For example, while monitoring social media activity, officers may observe inappropriate or illegal behavior. In other cases, an

officer may receive information reporting concerning online behavior from a collateral contact, a victim, or an anonymous source. In either scenario, the officer has a responsibility to actively research and verify the accuracy of information. Depending on the severity and urgency of behavior reported (e.g., a specific threat to an identified individual), the officer must take the appropriate actions in a timely manner to prevent harm. Failure to do so could create significant liability for the officer and/or the agency (Lyons & Jermstad, 2013).

THIRD-PARTY PRIVACY

While agencies may conclude that they have the authority and justification to examine a client's social media activity, the parameters beyond the client may be less clear. For example, agencies will need to determine in what cases, if any, it may be appropriate to monitor the activity of the client's online friends and associates (third parties). Some factors that may be considered include whether or not the other party is a criminal associate or co-defendant, whether there has been communication about a crime, or whether the client has absconded and may be in communication with the associate. To avoid unnecessary intrusion into associates' privacy, agencies need clearly articulated justifications for examining their activity as well as guidance to establish parameters regarding the associate profile review, such as reviewing only public areas and/or avoiding covert undercover actions (Shipley & Bowker, 2014).

POLICY DEVELOPMENT

As discussed, the use of social media monitoring is not without potential pitfalls. It is therefore imperative that agencies develop written policies to guide their operations on the appropriate use of this tool. While Global's 2013 document, *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations,* is focused on law enforcement operations, many of the principles outlined are helpful for community corrections agencies. For example, policy should be developed with the assistance of key stakeholders in the jurisdiction, such as judges, prosecutors, the defense bar, and law enforcement. Agencies should consider requiring all clients to disclose and update all of their email addresses and social media profiles as a standard practice, but not every client's activity needs to be scrutinized equally. Agencies should prioritize efforts on an individual, case-by-case basis, considering factors such as risk level and offense type (Bowker, 2012). Agencies and their officers also should be trained on techniques for searching online, using anonymization methods, collecting and authenticating online evidence, and keeping their equipment safe from malware (Shipley & Bowker, 2014). Finally, agencies should provide guidelines for responsible monitoring and the authorizations required for the various monitoring approaches.

Once implemented, the agency should regularly review and incorporate appropriate updates in its social media policy to ensure it remains current and reflects new state and/or federal requirements.

CONCLUSION

For better or worse, social media is a large and growing part of modern life. Its use is ubiquitous, particularly among younger generations. Community corrections agencies should understand that individuals under supervision maintain a virtual presence and what happens online can be as important as what goes on in the "real" world. Effective investigation and supervision, therefore, may require increased awareness of the social media landscape, greater appreciation for the potential value of the information that can be obtained, and knowledge of the available tools and techniques to monitor what clients are doing on social networking sites. Agencies are encouraged to explore the use of social media monitoring to support their mission. Nonetheless, agencies that move forward in this regard should carefully consider all policy implications and should develop guidance to ensure that officers use this tool in a responsible manner.

REFERENCES

Baldas, T. (2015, September 16). Ex-con back behind bars after posting photo on Facebook, *Detroit Free Press.* Retrieved from https://www.freep.com/story/news/local/michigan/detroit/2015/09/16/facebook-excon-parole/32521243/

Bernstein, M. (2012, June 23). Probation officer answers Facebook taunt, "Catch me if you can." *The Oregonian*. Retrieved from https://www.oregonlive.com/portland/index.ssf/2012/06/probation_officer_answers_face.html

Bowker, A. (1998). REDUCE: The six aims of financial investigations for probation officers, *Federal Probation*, *62*(1).

Bowker, A. (2011). Managing the risks posed by offender computer use. [APPA News]. *Perspectives, 35*(4).

Bowker, A. (2012). *The cybercrime handbook for community corrections: Managing offender risk in the 21st century*. Springfield, IL. Charles C. Thomas Publishers.

Bologna, G., (2018, October 10). Man arrested after posting Facebook video showing how to remove an ankle monitor, *Springfield News-Leader.* Retrieved from https://www.usatoday.com/story/news/nation-now/2018/10/10/man-removes-ankle-monitor-facebook-video-missouri/1587259002/

Buzzetto-More, N., Johnson, R., & Elobaid, M. (2015). Communicating and sharing in the semantic web: An examination of social media risks, consequences, and attitudinal awareness, *Interdisciplinary Journal of e-Skills and Life Long Learning, 11.* Retrieved from http://www.ijello.org/Volume11/IJELLv11p047-066Buzzetto1666.pdf

CBS (2018, March 20). Novato man on probation arrested after boasting about drugs on Facebook. Retrieved from https://sanfrancisco.cbslocal.com/2018/03/20/novato-probation-arrest-facebook-drug-boast/

Clear, T. R., & Cole, G. F (1990). *American Corrections, 2nd Edition*, Belmont, CA: Wadsworth.

Eiseman, J. (2010, November 22). Cops use Facebook to bust bragging criminal, *NBC-New York*. Retrieved from https://www.nbcnewyork.com/news/local/Bragging-Criminals-Caught-on-Facebook-by-Police-109892399.html

Freger, H. (2018, May 29). Law enforcement officials push for broader access to social media data. *ABC News*. Retrieved from https://abcnews.go.com/us/law-enforcement-officials-push-broader-access-social-media/story?id=55507706

Global Justice Information Sharing Initiative (2013) *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations*. Retrieved from https://it.ojp.gov/documents/d/Developing%20a%20Policy%20on%20the%20Use%20of%20Social%20Media%20in%20Intelligence%20and%20Inves....pdf

Gokavi, M., & Stewart, C. (2018, February 17). 2nd person charged with threatening juvenile judge on social media. *Dayton Daily News.* Retrieved from https://www.daytondailynews.com/news/crime--law/2nd-person-charged-with-threatening-juvenile-judge-social-media/c9QmvV8HhQYD865UF9aj9L/

Grimes, B. (2015, December 22). Man accused of threatening Ill. probation officer, *Effingham Daily News.* Retrieved from https://www.correctionsone.com/corrections/articles/56860187-Man-accused-of-threatening-Ill-probation-officer/

Haddad, K. (2018, July 31). Detroit felon faces new charges after posting gun photo to Instagram while on probation. *ClickOnDetroit*. Retrieved from https://www.clickondetroit.com/news/convicted-detroit-felon-faces-new-charges-after-posting-gun-photo-to-instagram-while-on-probation?utm_content=14026414&utm_source=Sailthru&utm_medium=email&utm_campaign=Headlines

Jones, W. (2014, March 27). Woman's Facebook post ousts her probation violation, *ClickOnDetroit.* Retrieved from https://www.clickondetroit.com/news/womans-facebook-post-ousts-her-probation-violation

Korn, P. (2015, July 16). Goodbye graffiti: Social media may be triggering gang violence *Portland Tribune.* Retrieved from https://portlandtribune.com/pt/9-news/266654-139442-goodbye-graffiti-social-media-may-be-triggering-gang-violence

Lyons, P., & Jermstad, T. (2013). *Civil Liabilities and Other Legal Issues for Probation/Parole Officers and Supervisors*, 4th Edition. Washington, D.C.: National Institute of Corrections.

Maas, D. (2018, September 24). Facebook warns Memphis police: No more fake "Bob Smith" accounts", *Electronic Frontier Foundation*. Retrieved from https://www.eff.org/deeplinks/2018/09/facebook-warns-memphis-police-no-more-fake-bob-smith-accounts

Matsakis, L. (2018, March 28). What to look for in your Facebook data – and how to find it. *Wired*. Retrieved from https://www.wired.com/story/download-facebook-data-how-to-read/

Mississippi Department of Corrections (2018). Facebook page, retrieved from https://www.facebook.com/MississippiDepartmentOfCorrections/posts/absconder-back-in-custody-mdoc-is-no-longer-searching-for-matthew-rutledge-13969/606835669492282/

Murphy, K. (2010, August 11). Web photos that reveal secrets, like where you live. *New York Times*. Retrieved from https://www.nytimes.com/2010/08/12/technology/personaltech/12basics.html

Peet, D. (2012, September 20). Social media analytics in law enforcement: Social media analytics can aid law enforcement and first responders in civil unrest, disasters and investigations. *Police* Magazine [Technology Blog]. Retrieved from http://www.policemag.com/blog/technology/story/2012/09/social-media-analytics-in-law-enforcement.aspx

Pew Research Center (2018). *Social Media Fact Sheet*. Retrieved from http://www.pewinternet.org/fact-sheet/social-media/

Pimentel, R., & Muller, J. (2010). The containment approach to managing defendants changed with sex offenses. *Federal Probation, 74*(2).

Rayborn, J. (2009). Innovative officer captures fugitives. *Corrections Today, 71*(3).

Russo, J., & Matz, A. K. (2014). The use of social media for monitoring defendants, probationers and parolees: Results of a survey of the APPA membership [Technology Update]. *Perspectives*, *38*(1).

Shipley, T. G., & Bowker, A. (2014). *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*. Waltham, MA: Syngress.

Surette, R. (2015). Performance crime and justice. *Current Issues in Criminal Justice*, *27*(2).

Sweeney, E. (2012, November 29). Probation 2.0: How technology is changing probation work. *Boston Globe.* Retrieved from https://www.bostonglobe.com/metro/regionals/south/2012/11/29/probation-how-technology-changing-probation-work-probation-officers-tap-social-media/Qtv52cQffcVbkAsJqcg6lK/story.html

Tanner, J. (2007). Beyond prosecution: Improving computer management of convicted sex offenders. KBSolutions, Inc. Retrieved from http://www.kbsolutions.com/beyond.pdf