American Probation and Parole Association

Issue Paper
on
The Use of Social Media
in
Community Corrections

Submitted by the Technology Committee

August 27, 2014

Introduction

This paper was developed to elevate the awareness of the potential of social media, also known as social networking, in the field of community corrections. Monitoring client[1] activity on social media can be an important component of the investigation or supervision process, however with opportunities come challenges. This paper will highlight the importance of establishing policies around social media use and identify some of the issues community corrections agencies may encounter as they incorporate social media in their investigation and supervision practices.[2] Specifically, the paper addresses four areas of interest with social media usage in community corrections: (1) client investigations and intelligence gathering; (2) policy development (3) available tools to assist agencies monitor social media; and (4) training resources.

What is Social Media?

The Merriam Webster online dictionary defines social media as "forms of electronic communication (as Web sites for social networking and micro-blogging) through which users create online communities to share information, ideas, personal messages, and other content (as videos)." Social media is the platform which allows users to engage with each other using the Internet to participate in, comment on and create content as a means of communication. Common social media sites include Facebook, Twitter, LinkedIn, Pinterest, Google+, Tumblr and Instagram.

Why is it Important to Understand Social Media and its Widespread Uses?

Print media is no longer a primary source of receiving information or distributing it. Over the last decade, technological advancements have allowed businesses and individuals to use free and fee-based Internet applications as a primary method of interacting with and engaging current and prospective customers, family members and friends. Social media has also made it much easier to find and interact online with others who share similar interests. All of this drives discovery,

[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.

[2] It is important to recognize the content of this paper is for informational purposes and intended to provide guidance to agencies. Identified web sites and/or software applications does not imply endorsement or support of them.

sharing, activism and influence. Through the use of social media, community corrections agencies can potentially track clients and their companions, view likes/dislikes, locate clients who have absconded, observe violations in real time and keep a better track of those under their supervision.

The Need for Guidance

As social media use has become pervasive in contemporary society, it is increasing imperative that community corrections agencies directly address the implications of this emerging communication method for the investigation and supervision process. Agencies both large and small are wrestling with ethical and professional decisions in an area with little to no history to provide guidance. If an agency decides to allow officers to use social media as an investigative or supervision tool, policies and procedures are needed to ensure that such practices are authorized, are used in a responsible manner, and consistent with the agency's mission and policy. Furthermore, social media is rapidly evolving and agencies will need to regularly examine and update their policies and procedures.

Social Media in Community Corrections

Community corrections agencies have been slow to embrace social media, particularly when compared to their law enforcement counterparts. According to a 2013 International Association of Chiefs of Police (IACP) Survey, 95.9 percent of law enforcement agencies surveyed use social media.[3] However, a 2012 American Parole and Probation Association (APPA) survey (with 399 respondents) found only 44.4 percent of respondents utilize social media in their agencies.[4]

[3] International Association of Chiefs of Police. (2013) *2013 IACP Social Media Survey*.
[4] Russo, J., & Matz, A. K. (2014). The use of social media for monitoring defendants, probationers, and parolees: Results of a survey of the APPA memberships (Technology Update). *Perspectives, 38*(1), 22-33.

In community corrections, the 2012 APPA survey found the following results.[5]

Uses of social media	Agencies using social media in this way
General agency information	47.1%
Fugitive apprehension	40.8%
Public outreach	34.6%
Observe/monitor client's online behavior	33%
Recruitment	14.1%
Resources for clients	12.6%
Other	3.1%

The Uses of Social Media

The IACP survey[6] found that law enforcement agencies use social media in a variety of ways in support of their operations.

Use of social media	Agencies using social media in this way
Criminal investigations	86.1%
Public notification of crime problems	74.3%
Community outreach/citizen engagement	70.4%
Public notification of emergency/ disaster-related information	69%
Crime prevention activities	66.7%
Intelligence gathering	66.1%
Public relations/reputation management	64.9%
Soliciting tips on crime	64.9%

The results of the 2012 APPA survey showed that of those community corrections agencies monitoring social networking sites, the following methods were employed.

[5] Russo and Matz, 2014.
[6] International Association of Chiefs of Police. (2013) *2013 IACP Social Media Survey Results*

Method	Agencies using social media in this way
View public pages looking for clients	91.4%
Periodically require the client to open his/her profile in the officer's presence to review	32.6%
Create an investigation identity to conduct covert online monitoring	28.8%
"Friending" clients to gain access to private pages	28.3%
Other	3.9%

Investigations and Intelligence Gathering

It is no secret that supervision officers are required to know quite a bit about their clients. The knowledge is first sought prior to conviction and sentencing, in the pretrial and presentence investigation processes. Later as part of the supervision process, officers must be aware of the conditions their clients are subject to and must monitor compliance. In the past, investigations and intelligence gathering focused on conducting interviews, obtaining paper reports/records and making frequent home and community contacts. However, today a significant percentage of the population has a social media presence and this includes, of course, persons under supervision. An estimated 78 percent of North American residents were online in 2012.[7] Facebook, the current social networking leader, had more than 930 million worldwide users on September 30, 2012.[8] Because more of a client's activities involve social media or an online profile, supervising officers and agencies need to move beyond the brick and mortar world and include the social media sphere as part of their standard investigative and supervision activities. Due to the volume and type of information supervising officers can learn about clients through social media, it is critical that agencies develop protocols on the proper use of this tool.

Issues Regarding Social Networking Investigations

One of the most compelling reasons for accessing a client's social media presence can be termed the "window into their personality" effect. Individuals post information online that is not otherwise normally disclosed to others. This information is frequently posted in public areas. By accessing social networking sites, officers can often find information about their clients not

[8] Internet World Stats. (n.d.) *Facebook Growth and Penetration in the World - Facebook Statistics - 2012*

normally available to them. Information posted in public areas does not require special authorization to access or review. Access to public areas does not require special subscriptions to intelligence databases.

There are, however, several concerns to venturing into social media, which need to be addressed.

Infrastructure & Security

In order to monitor social media use, officers must have the ability to access the Internet. This may seem obvious but not every agency allows their officers Internet access. The 2012 APPA survey found that 12% of respondents reported that they don't have access to the Internet for work purposes.[9] One reason for this is network security concerns correctly raised by agency information technology departments. Access to the Internet requires secure systems. Accessing the Internet from an unsecure agency computer can introduce malware that can compromise not only the investigation but the agency's main network. Some officers will use their personal devices and accounts to gain access not provided by their agency. Officers who use unsecure personal devices run the risk of exposing sensitive personal information.

Designating a computer(s) outside of an agency's network and providing it with separate Internet access, such as WiFi, is a good starting point. This avoids exposing the agency's entire IT systems to harm, as well as eliminates any risk to an employee's personal computer and information. However, separate access does not automatically translate into security. The designated computer software, including anti-virus and anti-spyware applications, must be maintained and kept updated. A firewall must be used and kept current. To ensure 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.

[9] Russo & Matz, 2014

Access to Information

Although much of what clients post online is in public areas, many are learning to post in less public areas or are restricting viewing access. As a result, officers will increasingly need to learn legal techniques for gaining access to these more private areas. Specific techniques and sources of training are discussed later in this paper. Agencies also need to realize that for those clients whose computer use must be managed more closely, such as those accused or convicted of sex crimes, other techniques are required[10], including searches, computer monitoring and polygraph tests. Some supervising officers may consider creating a fictitious profile on a social media site for the purpose of client surveillance. However, it is a common requirement the profiles created on social networking sites are for real people. Consequently, agencies and supervising officers must be knowledgeable about these policies and ensure they comply with them.

Authentication of Information

Other concerns are the nature of *online electronically stored information* (OESI) and its authentication, which has two components. Information stored online is easily altered or deleted. It is also subject to alteration or destruction after collection. Authentication requires officers collect and preserve OESI in a manner establishing that what they collected is what they saw online and was not altered after collection. This establishes a "chain of custody" for OESI for use in any legal proceeding. Officers need to learn about and use tools and techniques that establish this "chain of custody" for OESI.

The second component of authentication requires officers to gather information supporting that the OESI they collected is "what it purports to be." There must be evidence beyond just the OESI supporting that the information collected is an actual representation of what occurred.

[10] Bowker, A. (2011) "Managing the Risk Posed by Offender Computer Use" ***Perspectives***, 35(4), 40-49.

A Case for OESI

In ***Griffin v. Maryland***, (19 A.3d 415, 419 Md. 343), the Maryland appeals court ruled MySpace pages were erroneously admitted into evidence because they had not been properly authenticated. The postings were admitted by the trial court 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 appeals court ruled these factors were not sufficiently "distinctive characteristics" to properly authenticate the pages. The court ruled the presented profile printouts and posting as provided could not rule out the possibility someone other than the defendant could have made the profile or had access to it to make the posting. This case and others reflect the need for officers to provide evidence supporting that OESI is what it purports to be, which can be done. For example, an admission or confession from the client may be used to authenticate OESI. Additionally, digital evidence found during a computer or cell phone search may also be used to authenticate OESI. With proper collection procedures meta-data may also help authenticate OESI.[11]

Privacy

The final concerns with social media investigations are what can be termed *mission creep* and privacy. Mission creep refers to the incremental and often unintended and unauthorized expansion of an agency's mission into new and uncharted areas. Clearly, a client's social networking profile can be examined as part of the pre-sentence or supervision process. But how far should the examination extend? Does it include examining and documenting all their connections to others or just those who are "criminal associates?" Sometimes a client will set their profile to "private" but their associates might not be so diligent. Is it appropriate to check their associate's profiles for information pertaining to the client? The client is under supervision; however the clients'

[11] Some methods, such as printing hard copies, will not capture hyperlinks or metadata that may be present in the OESI. These additional pieces of data may be important to help prove the OESI is what it purports to be. There are both free and paid software that can be used to capture OESI. Many of these programs provide for the date and time of the capture to be included in the file name. Additionally, there are free programs that will "hash" or fingerprint the captured data to insure the integrity of the captured OESI.

associates may not be. These questions raise important issues that should be addressed by all agencies to ensure that operational practice remain in alignment with mission and policy.

General Principles for Social Media Activity

Agencies need clear justifications for examining social media activity beyond merely stating it is part of a client's supervision. Justifications need to be articulated for both clients and their associates. Client-specific justifications[12] generally fall in the following categories: Pre-sentence Report Preparation; Supervision and Violations; and Officer Safety.

Client-Specific Justifications

Pre-trial/Pre-sentence Investigation and Report Preparation

Investigative reports provide a court with background on the client to assist in making critical decision such as pretrial release, sentencing and juvenile court dispositions. A constant concern about these reports is whether they accurately portray the person before the court. Some of the types of questions courts grapple with are:

- Is the person truly remorseful for their delinquent/criminal conduct?
- Is the person being honest about not having a substance abuse problem or a gang association?
- Has the person disclosed complete and accurate information about all their assets?

As part of the pre-trial or pre-sentence report process, social media investigations have the potential to reveal information that may contradict the image the convicted person is trying to convey to the judge.

Supervision and Violations

[12] Many of the client justifications noted are valid as well for agencies involved in pretrial supervision. However, justification for their use in a pre-conviction setting may need to be further defined, consistent with the pretrial function.

Social networking site investigations can and have detected OESI on a client's profile that provides evidence of both technical and new law violations. Below are some common examples of violations officers have discovered while reviewing clients' activity on social networking sites. They may be helpful for agencies working to articulate justification for this type of investigative tool. It is by no means an exhaustive list.

1. Internet Restrictions -- Some clients, such as those convicted of sex crimes, may be precluded by conditions or statutes from accessing social networking sites. Others may be prohibited from using the Internet at all while on community supervision. Searching for such a client's profile and investigating possible matches have detected violations of these online restrictions. Special software is available that allows agencies to remotely monitor clients' use of social networking sites. The 2012 APPA survey found 28.8 percent of respondents that monitor client social media activity used software-based monitoring tools.[13] This software is typically installed on a client's computer and monitors sites they visit. This is a particularly useful tool when monitoring individuals accused or convicted of sex offenses.

2. Criminal/Gang Associations: Standard supervision conditions preclude clients from associating with co-defendants, convicted felons or other persons deemed inappropriate. Other clients may be involved in gang activity. Checking social media site activity can provide some information as to the client's compliance with these directives. Clients are frequently caught associating with one another on social media sites as well as freely displaying gang signs or colors.

3. Substance Abuse -- Clients will sometimes reference their drug and/or alcohol usage in posts to social media sites, which may include pictures or references of drug use and their friendship with known drug users. Some clients seek out information on how to defeat drug testing with their posts on social media sites. Confronting clients with this information may help them seek treatment. For those

[13] Russo & Matz, 2014

already in treatment, it is an issue that needs to be addressed during counseling. For those who are not amendable to treatment, an administrative sanction may be justified.

4. Unauthorized Leave -- Some clients will post images of themselves traveling or vacationing outside of a jurisdiction without permission. Others on home confinement restrictions, will post updates reflecting 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 geo-location data to the post. This information, if available, can be very important particularly if the context of the image leaves some doubt about actual location (e.g. a picture of the Eiffel Tower – is it in Las Vegas or Paris?). The geo-location data embedded in a post or image removes this doubt.

5. Criminal Behavior -- Clients may post threats on social networking sites. Targets of these threats runs the gamut from former significant others to informants, witnesses and even law enforcement officers and/or agencies. Clients have also posted pictures of themselves posing with firearms or bragging about a criminal act, such as a robbery recently committed.

6. Other Non-Compliance -- Social media activity may show the client with unexplained assets, such as the display of money. Some clients post pictures of themselves "goofing-off" at work, jeopardizing their compliance with employment conditions.

7. Fugitive Apprehension -- Social networking sites have been extremely helpful for locating absconders from probation or parole. Absconders often maintain their social media activity even while seeking to elude authorities. The contacts, status updates and pictures they post (and associated geo-location data) are invaluable clues to apprehension. Many law enforcement agencies effectively use social media to invite and receive help from the community to identify suspects,

apprehend fugitives and solve crimes. Some agencies list wanted bulletins on their website, while others have a Facebook and/or MySpace page. Some police departments use YouTube to share surveillance videos showing suspects committing a crime in order to generate leads from the public to identify the suspect(s). In community corrections, the Kentucky Division of Probation and Parole uses MySpace, Twitter and Facebook to locate clients in a warrant status. The agency's MySpace page[14] shows client photos and their crimes, contact information and an interactive map of the state's counties that displays wanted persons. The site includes updated blog posts sharing the status of apprehended individuals, a Frequently Asked Questions (FAQs) section and contact information to report wanted persons.

Officer Safety

Officers are able to glean information from a client's social media activity that can be vital to their personal safety. For example, clients may post information about the weapons they have access to; the fact that they are trained in hand-to-hand combat; they have animals in the home; or have violent associates and/or use drugs. Some clients comment about or post threats about officers. Social networking sites, such as Twitter, may give officers an overall understanding of the community, particularly after a recent significant news event. Some larger supervision agencies may consider using social media monitoring tools, which gather data and provide information on trends in a particular area.

Non-Client Justifications

To avoid *mission creep,* agencies need clearly articulated justifications for examining the profiles of their clients' associates. The justification also reduces issues regarding the privacy of the associates. Part of the justification should include supervisor approval before an officer begins reviewing the profiles of a client's associates. If supervisory approval is given, the officer must have specific parameters guiding the associate profile review, such as reviewing only public areas and/or avoiding covert undercover actions.

[14] Kentucky Probation Fugitives - https://myspace.com/ky_pandp_fugitives.

Two clear justifications are: (1) the client's associate is a co-defendant or felon, or (2) the associate has communicated with the client about a supervision or criminal law violation. Monitoring associate profiles of absconded clients may also be justified provided there is a clear relationship between the two beyond just social media interaction.

Monitoring Methods

A policy guide developed by the Bureau of Justice Assistance (BJA) with the support of the Global Justice Information Sharing Initiative Advisory Committee (GAC) and the Criminal Intelligence Coordinating Council (CICC)[15] notes three methods of accessing social networking sites by law enforcement: *Apparent/Overt Use, Discrete Use* and *Covert Use*. Each method has a different level of intrusiveness.

Apparent/Overt Use

Apparent/Overt Use involves accessing of social networking sites without any interaction with the target. 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 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. This method has a low level of intrusiveness as the information accessed is in public areas.

Discrete Use

Discrete Use involves techniques concealing the officer's identity but no online interaction with the client. 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. When an officer visits a website, the browser provides an IP address, along with

[15] Global Justice Information Sharing Initiative (2013) *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities Guidance and Recommendations.*

other information, so the officer can view the website. The individual controlling the website can capture this information, which can be used to identify the officer (or visitor), their Internet service provider (even government providers), information about their browser, and other information. This same functionality is available with some social networking sites and allows the creator of the social media account to learn who is viewing their social networking page(s). Web anonymizers, such as Anonymouse.org (http://anonymouse.org/anonwww.html), act as a go-between the user (an officer) and the target website (the client's social networking page(s)). The target website only sees information provided by the web anonmyizer and not the user. In this way, the user conceals that they are viewing the website.

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. For instance, one might create a fictitious identity to access the public areas of an adult-oriented dating site to determine if a client charged with a sex crime has created a profile on the site. In this case, the fictitious identity is created not for interaction with the target but to view public areas. If the user created a truthful identity they would be revealing themselves to all other members, something the user likely would not want to occur. In some cases using both a fictitious identity and an anonymizer might be called for to conceal one's identity not only from the social networking site's membership, but also from the website operators.

Covert Use

The most intrusive method is Covert Use and this requires special training, equipment and specific authorization. This method involves concealing the officer's identify and requires online interaction with the client to gain information and/or evidence of a violation. It may also involve the use of search warrants, to obtain access to a client's account.

Knowledge of online role playing should not be confused with the skills needed for covert investigations. They are not the same. Corrections must have a legitimate purpose

and authorization for creating a fictitious profile and they must be prepared to document their efforts. Additionally, officers must be extremely careful to not use a real person's name to create the fictitious identity. There can be serious repercussions for the real person if something goes amiss during the investigation, creating a civil liability for the agency. For instance, creating a profile using the name of an individual's known associate to locate the client may subject the real person to harm. If this approach is used, the agency must have full understanding of the social networking site's policies about the creation of profiles. Many sites prohibit creating fictitious profiles and if discovered the site will delete the profile without advance notice to the creator.

Review with Client Cooperation

One additional investigative method available to community corrections but not law enforcement is the ability to require clients to provide access to their profiles. Standard supervision conditions usually require clients to permit officers to visit them at home or place of employment or "elsewhere." In this case "elsewhere" can be the virtual world of social media. In cases where such rules do not exist, establishing such conditions would allow such access. One important caveat is warranted. Officers must be diligent in obtaining disclosure on all social media profiles used by an offender. Requiring written disclosure of all social media profiles is important. Such disclosure should also require information on all email accounts used by the offender, which is usually the first step in setting up a social media profile. Officers should also be aware that this information will likely need to be updated. Other methods for detecting additional undisclosed social media profiles, are third party contacts, computer searches, Internet searches, and inquires with various paid data brokers. One additional, the use of polygraph testing is also available for sex offender cases.

Once a client's profile has been identified, officers can request their client 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 requiring the client to access their social media profile in the officer's presence for a review, which would include information in the public locations and that which the client has 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. Additionally, this method requires the officer to visit the profile in the client's presence, creating possible safety concerns. Some social media sites, such as Facebook and Google, permit the download of the entire user's activity, which can be reviewed later by the supervision officer.

Client provision of their social media user names and passwords to their officer creates legal concerns, such as chain of custody and data integrity issues. Those concerns relate what the officer may do with that access. For example, did the officer use the access to post messages or send emails or open recently received emails? Or, did the officer later access the account after the initial authorized review? Depending upon the action taken, an officer may be committing a criminal violation (Unlawful Access to Stored Communications, 18 U.S.C. § 2701). Standard policies and procedures do not require clients to give the keys to their home so their officer can visit the home when the client is not there. "Visits" to monitor social media activity should follow the same rationale. Therefore, the best solution is to require the client's presence for such reviews.

Development of a Social Media Policy

For agencies monitoring social media as an investigation or supervision tool, it is imperative to have a written policy to guide their operations on the appropriate use of this tool. The policy should be developed with the assistance of key stakeholders in the jurisdiction (e.g. judges, prosecutors, defense bar, law enforcement). The 2013 IACP Social Media survey found 69.4 percent of the law enforcement agencies surveyed have a written social media policy, 16.3

percent did not and 14.3 percent were in the process of developing one.[16] The 2012 APPA survey found only 26.1 percent of respondents' agencies have a social media policy.[17] Further inquiry revealed that the policies focused on employee use of social media primarily in their personal lives and not as a supervision tool.

Community corrections agencies need to develop sound policy for conducting investigations and supervision using social media. Agencies are encouraged to require all clients to disclose and update all of their email addresses and social media profiles as a standard practice. This should not suggest that 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 considering factors such as risk level and offense type. Agencies and their officers also are encouraged to become acquainted with techniques for online information searching techniques, anonymization methods, collecting and authenticating online evidence and keeping their equipment safe from malware (viruses, spyware, trojans, etc.).

The Global Justice Information Sharing Initiative document, *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities*[18] is an excellent resource. The document provides seven well-reasoned elements for law enforcement agencies to consider when developing a guide to intelligence and investigative activities in a social media environment. The elements listed below also make sense for community corrections with the unique caveats noted previously:

1. Articulate 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 networking sites or tools is authorized (as well as use of information on these sites pursuant to the agency's legal authorities and mission requirements).

[16] International Association of Chiefs of Police. (2013) *2013 IACP Social Media Survey Results*.
[17] Russo & Matz, 2014
[18] Global Justice Information Sharing Initiative (2013) *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities Guidance and Recommendations.*

3. Clearly define the authorization level(s) needed to use information from social networking 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 reason(s) and purpose(s), 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 used for an authorized law enforcement purpose.

7. Identify dissemination procedures for criminal intelligence and investigative products containing information obtained from social media sites, including appropriate limitations on the dissemination of personally identifiable information.

Another resource for policy development is IACP's Center for Social Media (http://www.iacpsocialmedia.org) which was created in 2010 in partnership with the Bureau of Justice Assistance. The Center serves as a clearinghouse for information and free resources for law enforcement personnel to develop or enhance their agency's use of social media and integrate Web 2.0 tools into agency operations. The stated goal is to build the capacity of law enforcement to use social media to prevent and solve crimes, strengthen police-community relations, and enhance services. This site includes information on developing a social media policy, technology, topics of interest, and resources.

Specific publications of interest include:

- *Social Media Concepts and Issue Paper*
  http://www.iacpsocialmedia.org/Portals/1/documents/social%20media%20paper.pdf

- *IACP Social Media Model Policy*
  http://www.iacpsocialmedia.org/portals/1/documents/social%20media%20policy.pdf

Once implemented, it is important to periodically review and/or update an agency's social media policy to ensure it remains current and reflects new state and/or federal requirements. It is suggested that these policies be reviewed annually at a minimum.

Tools Available to Assist Agencies in Monitoring Social Media

When monitoring a client's social media activity the Internet has most of the needed tools. The list below identifies some tools and their general capabilities and limitations.

- Google (https://www.google.com/)

  Searching with google.com can produce a variety of results for any given client. The quality of the search results depend on the criteria entered. Learning how to use Google Boolean Operators can improve the relevance of the search results.

- Facebook Visualizer (https://www.lococitato.com/facebookvisualizer/)

  This application must be installed on the officer's computer and is for Law Enforcement use only. There is an annual license of around $40. The application can track up to 10,000 connections to a Facebook profile. It then displays the connections on a map showing how each profile is connected.

- MixMap.com (http://www.mixmap.com/)

  MixMap Tracker can be a useful tool for agencies that permit officers to create undercover profiles. This tool works on LocoSpace and MySpace. It allows officers to track who visits the officer's undercover profiles by logging the IP address of the visitor. Having the IP address, the officer can learn the rough geographic location of the visitor. Again, the use of undercover profiles must be carefully considered and if used, specific policies and procedures should be developed to govern its use.

- SEARCH Social Networking Custom Search Engine

  A search engine designed to specifically search various social networking sites for investigative keywords. The social networking websites currently included are: Facebook, MySpace, Google+, Tribe.net, LinkedIn, and meetme (formerly myYearbook). http://www.google.com/cse/home?cx=003390515112872459514:tuv0s6zg5lg&hl=en

- Wayback Machine

  The Internet Archive (http://archive.org/) Wayback Machine is a service allowing people to visit archived versions of Web sites. Visitors to the Wayback Machine can type in a URL, select a date range, and then begin surfing on an archived version of the Web. The Wayback Machine can be useful if a client deletes online content and the officer wants to visit and review an older version of a website to research a past post.

- Watchthatpage.com (http://watchthatpage.com/)

WatchThatPage is a service allowing officers to automatically collect new information from favorite web site pages. Officers select which pages to monitor and WatchThatPage finds the changed pages and collects the new content. The new information is emailed to the officer and/or a personal web page. Officers can specify when to collect page changes, so they are fresh when reviewing them. The service is free.

- Other useful websites to consider include:
  - Whos Talkin (http://www.whostalkin.com/)

    Aggregates posts for a search term across blogs and social media platforms. Aggregation can also be limited to a particular platform.

  - GeoChirp (http://www.geochirp.com)

    Geochirp is a mashup between Twitter and Google Maps. It allows officers to select an area on a map, choose a radius, and view tweets emanating from that location in real-time. Officers can include keywords in the search to see only those tweets using the keyword. Geochirp is an excellent tool for monitoring Twitter during the conduct of search and arrest warrants or other law enforcement operations. Officers will need to use a Twitter account to use this website.

  - Trendsmap (http://trendsmap.com/)

    Trendsmap is continuously tracking Twitter trends and uses the location on users' Twitter profiles to map tweets to a geographic location. Since users' geolocation information is self-ascribed it may not be accurate.

Training

As technology becomes more pervasive it is only logical for persons under supervision to begin using it to manage their everyday lives. For some, the technology provides an opportunity to commit new crimes. Digital evidence considerations are no longer just a matter for law enforcement first responders and high-tech crime teams. It is imperative that those charged with community supervision have proper training to monitor their clients' use of technology successfully. Yet, officers across the country have vastly varying skill sets in digital evidence retrieval and recovery. While some agencies provide initial and on-going training covering technology and digital evidence, many other agencies have either sporadic training or no training at all. Meanwhile, the training officers do receive from different agencies and training organizations across the country is disparate.

Many officers today consider themselves "technologically savvy." Many have grown up with the use of mobile devices, computers and social networking sites. However, using social media and effectively collecting digital evidence from social media sites are very different skill sets.

Training Resources

There are numerous resources available for social media training. Although not an exhaustive list, this section provides a sample of the resources available to community corrections professionals wishing to gain skills and abilities to monitor their clients' use of social media.

1. FBI Regional Computer Forensics Laboratory

   The Laboratory website hosts a free webinar on "Digital Forensics & Social Media Evidence"
   http://www.rcfl.gov/DSP_T_webinar13summary.cfm

2. Fox Valley Technical College- National Criminal Justice Training Center

   The Training Center provides social media site training in its *Undercover Chat Investigations course*. The hands-on training takes place in a computer lab, which allows officers to develop their skills.

   This training is open to state, local and federal law enforcement to include corrections. State and local agency registrants must be a member of a regional ICAC Task Force or Affiliate Agency.
   http://www.ncjtc.org/ICAC/Courses

3. International Association of Chiefs of Police (IACP) – Center for Social Media

   The IACP Center offers training and technical assistance through its website. This no-cost technical assistance option provides services on social media account creation, social media strategy development and general social media consultation.
   http://www.iacpsocialmedia.org/Resources/TrainingTechnicalAssistance.aspx

4. SEARCH Group, Inc. – High-Tech Crime Training Services (HTCTS)

   The HTCTS training team provides *Online Investigations: Tools, Tips and Techniques* training course. This two-day course is non-technical in nature and officers with any skill

level to gain the knowledge they need monitor their client's use of social media. This hands-on course provides training on the major social media sites and some of the other non-mainstream social networking sites.

In addition to providing an in-person training course, SEARCH provides an eLearning (or online) training block in social media that is currently free for law enforcement agencies. This training block discusses the operation of the major social media sites, and some resources for conducting searches across the networks.

SEARCH also provides a technical assistance program. If officers have questions regarding how to search social media, capture evidence from a social networking page or how to serve legal process to the social networking site, they can contact SEARCH for assistance. Contact the SEARCH HTCTS team at www.search.org/programs/hightech

5. United States Secret Service – National Computer Forensics Institute

   The Institute provides training titled *"Online Social Networking."* During this four-day course, officers gain hands-on experience with social media investigations. This course provides instructor-led discussions and practical exercises to teach methodologies and techniques used during investigations.
   http://www.ncfi.usss.gov/catalog.html

This is not an exhaustive list of training. A simple Internet search using the keywords "Law Enforcement Social Networking Training" lists many of the resources identified above as well as others. The most important factor to consider when looking at using a training provider is to ensure the techniques presented comply with the agency's policies regarding the use of social media.

Conclusion

For better or worse, social media is a large and growing part of modern life. Community corrections agencies need to recognize that their clients maintain a virtual presence and what happens online can be very important. Effective investigation and supervision, therefore, require an understanding of social media, an appreciation for the potential value of the information that can be obtained, and knowledge of the available tools and techniques to monitor what their clients are doing on social networking sites.

While officers may be well-versed in social media in their personal lives, monitoring client activity as part of the supervision process is another matter altogether, one fraught with potential

pitfalls. Agencies must develop strong policies to guide officers who engage in this effort. Policies should address a multitude of issues such as such as network security, the nuances of online electronically stored information (OESI), privacy issues and acceptable investigation methods.

Agencies that choose to ignore their client's social media presence miss looking into a "window of their personality", which may reflect serious non-compliance or behavior that places the community a risk. Casting a blind eye to social media may place an agency in a precarious liability position if their client's online behavior becomes real world criminal conduct that could have been prevented. With the proper protocols in place, social media monitoring can provide a very powerful investigation and supervision tool. Agencies simply cannot afford to operate in the 21st Century and without these new tools.

References

Bowker, Arthur. (2011) "Managing the Risk Posed by Offender Computer Use" *Perspectives*, 35(4) 40-49

Global Justice Information Sharing Initiative (2013) *Developing a policy on the use of social media in intelligence and investigative activities: guidance and recommendations*. https://it.ojp.gov/gist/132/Developing-a-Policy-on-the-Use-of-Social-Media-in-Intelligence-and-Investigative-Activities--Guidance-and-Recommendations-

Griffin v. State of Maryland. 19 A.3d 415, 419 Md. 343. Court of Appeals of Maryland (2011)

International Association of Chiefs of Police. (2010) *Social Media: Concepts and Issue Paper*. Alexandria, VA: author. http://www.iacpsocialmedia.org/Portals/1/documents/social%20media%20paper.pdf

International Association of Chiefs of Police. (2010) *Social Media Model Policy*. Alexandria, VA: author. http://www.iacpsocialmedia.org/portals/1/documents/social%20media%20policy.pdf

International Association of Chiefs of Police. (2013) *2013 IACP Social Media Survey Results*. Alexandria, VA: author. http://www.iacpsocialmedia.org/Portals/1/documents/2013SurveyResults.pdf

Internet World Stats. (n.d.) *Facebook Growth and Penetration in the World - Facebook Statistics - 2012.* Retrieved May 8, 2014, from www.internetworldstats.com/facebook.htm

Internet World Stats (n.d.) *North America Internet Usage Statistics- 2012*. Retrieved May 8, 2014, from http://www.internetworldstats.com/stats14.htm

Kentucky Probation Fugitives. (n.d.) Retrieved May 8, 2014, from MySpace website https://myspace.com/ky_pandp_fugitives

Russo, Joseph & Adam K. Matz. (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), 22-33.