

Using Social Media as an Informant

Justin K. Crawford

Michigan State University

Abstract

With today's means of communication and the billions of people across the globe using social media, it is no surprise that law enforcement intelligence operations have turned to using social media as an information collection medium. Using social media to collect information on individuals offers many benefits to law enforcement agencies but also includes certain manageable risks. There are several oversight regulations that department administrators and officers alike should be aware of. While the regulations certainly do not prevent information collection, law enforcement officers may find the constraints somewhat burdensome. This paper seeks to help identify the more prevalent issues with using social media as a virtual informant and guide agencies in a way to avoid the more common mistakes. These mistakes can lead to civil rights infringements and government oversteps by state, local and tribal officials.

As societies continue to develop and the number of people with access to mobile devices increases, social media use continues to grow in parallel. These devices, coupled with third-party applications offer individuals a constant stream of user information and a medium to share second by second updates with anyone in the world. As the evolution of communication continues to shape and change the country, law enforcement officers and agencies must change the way they collect and analyze information. Today's law enforcement officers are increasingly facing asymmetrical threats including gang violence, organized crime, terrorist attacks and even violent attacks directed specifically at police that pose new and difficult challenges. They require not only looking at and analyzing information from organized gang and crime syndicates, but also terrorist organizations and homegrown violent extremists (HVEs). This is an incredible task that has pushed the idea of community policing into its newest edition of intelligence led policing (ILP). In addition to the complexity of crimes, today's terrorist organizations are increasingly advocating for the lone wolf to carry out attacks without specific direction from any central authority. This is done to avoid detection or denial by law enforcement and the national security intelligence community (IC) and to lessen the chance of disruption. To address these ongoing threats, ILP has the ability to utilize social media and other public forums to collect information in an attempt to identify, qualify and quantify specific threats. Social media intelligence or SOCMINT as designated by Omand, Bartlett and Miller (2012), is open source information that has the potential to identify suspicious activity prior to the threats materializing or provide insight into who may be responsible for past crimes already committed. Collecting information from social media sites carries many benefits but also the inherent concern of law enforcement abuses and how the collected information may be used. The line between what is private and public information is not always clearly defined and varies depending on the social

media platform being used. Adding additional complications to this process is how the user has their privacy setting applied or how the social media site has instituted default privacy settings. Despite these concerns, collecting information from open-source social media sites and applying an analysis process to the information offers an abundance of intelligence that can benefit many state, local and tribal law enforcement (SLTLE) agencies. After the analysis process has been applied to the raw information collected from a specific site or sites, the goal of law enforcement intelligence (LEI) operations is to create actionable intelligence products used to identify and mitigate threats to the public. These benefits outweigh the risks if certain regulations and standards are applied but nevertheless, privacy concerns need to be considered while implementing a SOCMINT process within any agency.

The law enforcement intelligence community currently collects information from an assortment of open sources including a variety of new and emerging technologies. This information is available to the public and therefore law enforcement. According to research from November, 2014 by LexisNexis, approximately 81% of Law enforcement officers use social media as a tool during investigations. Additionally, 73% of law enforcement officers that were surveyed believe that social media, when used as an investigative tool, can help solve crimes more quickly (LexisNexis, 2014, p. 2). This is not surprising as most people have social media accounts including police and it is an easily accessible medium to collect information. Rather than having to schedule meetings with potential witnesses or informants, the officer or analyst can simply use the computer at their desk and access any social media sites they have created accounts for. Although there is no guarantee the information they are looking for is available through open-source means, many times this is the case. This type of analysis should by no means take the place of meeting with people and interviewing witnesses. It should be used

as an additional tool to further vet already known individuals or discover new individuals that might have pertinent information who should be questioned. This method of social media collection is only going to increase as more and more individuals begin using these mediums to communicate with friends and family. Additionally, as mobile technologies continue to make it easier to feed the social media frenzy, the amount of information available will continue to grow. People in general, including criminals and police officers often forget that social media is open to the public (depending on privacy settings) and a record of posts, tweets and uploads remains associated with the user for what many would consider forever. This information, when privacy settings are not properly set, either intentionally or mistakenly, can offer valuable information to authorities for use in criminal cases.

The benefits of surveilling and analyzing social media sites are extensive especially with the promotion of attacks by HVE and lone wolf actors. These lone wolf attacks are almost impossible to identify, but if there is a sudden increase in social media traffic within a city limit, it can offer police advanced warning. According to Hollywood, Strom & Pope (2009, p. 3, 4), there are three initial clues that have been present in many of the recent foiled terrorist attacks. These include discovering clues during police investigations, direct reports to law enforcement and reports of suspicious activity that may indicate terrorist activity. Additionally, there is a history of arrogant criminals that have posted on social media sites bragging about the crimes they have committed. Recently, several members of a hate group called the Crusaders were apprehended in Kansas plotting to blow up a Somali refugee apartment complex (Berman, Larimer & Wootson Jr., 2016). On several occasions, these individuals posted hate messages and expressed discontent for the group of people they were targeting prior to their arrest. According to Hollywood et al. (2009), a review of 25 foiled terrorist attacks identified that, “80%

of the initial clues came from observing, reporting, and properly acting on behavior of concern, including both directly threatening behavior (such as openly discussing plans for terror attacks) and suspicious activity (such as conducting target site surveillance)” (p. 15). Law enforcements use of social media can easily contribute to the collection and validation of these types of threatening posts, tweets or uploads. Even though the posts might be covered under free speech protections secured by the Constitution, it allows law enforcement the ability to observe individuals in a way they would not have been able to 50 years ago. Information can now be obtained from social sites including pictures documenting equipment, personal associations with individuals and/or groups of people, other assets needed or used in a crime, messages between key people, geotagged information identifying location history and many other data points that when combined and looked at as a whole, may provide the evidence needed to prevent an attack or crack an existing case. This information can be identified, documented, analyzed and retained in an intelligence database by police for use in criminal proceedings as long as several regulations and restrictions are followed that will be discussed later.

In June, 2016, Facebook saw an average of 1.03 billion active mobile daily users (Facebook, 2016). That’s just counting the individuals using mobile devices to access their accounts and not users using their desktop or laptop computers. The amount of information passing through Facebook alone is almost incomprehensible. Add Twitter, Instagram, Snapchat and YouTube and the statistics are even more overwhelming. However, there are several technologies available that allow police agencies to identify specific criteria that might interest them and conduct targeted searches for information that might pertain to a crime they are trying to prevent. These programs allow intelligence teams to input specific data, including names, keywords or locations they are interested in and conduct a targeted search within a geographic

area or timeframe. It allows intelligence officers the ability to take a seemingly incomprehensible situation with millions if not billions of data entries, apply basic internet search skills, and these programs will sift through the millions of data points to provide a comprehensible output that is logical, easy to understand and on occasion provides actionable intelligence the law enforcement department can use. One such program that provides this type of social media datamining service is Snaprends. Snaprends (2016) details the ability of their program and describes it on their website as follows:

Snaprends simplifies the process of filtering through the vast social universe to find what matters to you. Our proprietary algorithms and processes paired with the ability to focus searches based on social networks, locations and keywords ensures you hear the full spectrum of social conversations.

Programs like Snaprends give police departments helpful tools they require to turn social media information into actual intelligence products similar to any informant that a police agency would historically have used to provide detailed situational information. Although Snaprends does not advertise their pricing on their website, an article from 2014 stated the software package costed \$4,200 at that time (Spoto, 2014). This was based on a city police departments request for funding to purchase and implement the Snaprends software package. This seems to be a reasonable price for most departments to afford based on the time and effort the program saves analysts by compiling huge amounts of information into an efficient data package. Another similar program is Signal. Signal's website (2016) describes the following:

Signal is a cloud-based Open Source Intelligence platform, designed to make the job done by public safety agencies easier and more efficient by saving operational teams time and money.

Both of the listed programs track and document many details of public social media posts. As mentioned above, this information can include critical pieces of information including but not limited pictures, posts and even location information with the use of geotagged information. This real-time monitoring technology allows police to view and track information about crimes, criminals and even victims. It has the ability to establish the who, what, when and where clues that officers are desperately trying to put together in order to solve past crimes and try to interpret future actions by individuals. The software also allows police to track, monitor and document the social media activity of known criminals. Known criminal information can be entered into the software and can monitor in real time any interaction the individual has with several social media sites. Even the ability to track and establish personal relationships is advertised. This can be used to identify additional participants that cooperated to commit a crime or other criminal action. The use of this technology can be coordinated with other departments through the use of fusion centers. With each local department responsible for their own particular city, county or state, the department could then feed relevant intelligence to the nearest fusion center. With this additional intelligence, the fusion center could analyze and determine if there is crime overlap and determine the appropriate action that needs to be taken. This could also be used to identify potential HVE or other terrorist groups working together. If one individual posts a particular social media message and another individual across the state posts the same hate filled language, there could be an identifiable commonality between the two individuals thus allowing LEI officers to identify potential conspirators either before or after an attack.

SOCMINT operations also offer law enforcement intelligence teams a unique opportunity to not only collect information for analysis, but also the opportunity to have two-directional

communication with the public in almost real-time. It seems today that many people, especially younger generations, are reluctant to call anyone and have verbal conversations with them. It would seem logical that this hesitation would also carry over to the younger generations interaction with the police when reporting suspicious incidents or unusual behaviors. Someone might see something suspicious they want to report, but they might be hesitant to call 911 and report what they saw thinking it is not really that big of a deal. However, social media allows these younger generations to communicate with law enforcement through messaging applications such as Facebook and Twitter. As a result of this two-way communication, LEI can collect information and they can also ask for the public's assistance when certain situations develop. This type of communication has already been implemented by many police agencies. According to LexisNexis (2014) research, "More than a third (34%) now notify the public of crimes via social media, up 11% from 2012" (p. 3). AMBER alerts (America's Missing Broadcast Emergency Response) are a well-known example of this type of communication. These alerts are now text messaged to cellular phones within a specific geographic area, broadcast across social media sites and even displayed on interactive highway signs. There are also several mobile technologies that allow law enforcement to collect and track real time information for use in these situations. Facebook, Instagram and Twitter are just a few popular options that are available to law enforcement. Nextdoor is one such recent addition to the social media application list. Nextdoor is a neighborhood watch application that allows citizens to share information with their neighborhoods including their local law enforcement departments. Users can upload pictures of suspicious vehicles, people going door to door soliciting illegally and communicate any threats that might be happening in their neighborhood through an urgent message system. Additionally, local law enforcement can receive, collect and distribute

information shared by citizens in nearby neighborhoods. This application can be used to share information either identifying a wanted person of interest or suspect in a crime and can be targeted to geographic localities where the individual was last seen. Another example of an added benefit of communication via social media is that social media sites can be used to provide educational bulletins to the public with specific instructions regarding what kind of suspicious activity should be reported to law enforcement and how to report it. Finally, trends in crime and other challenges the police are experiencing can be easily communicated. Public information officers can communicate specific examples of the crimes that have been recently committed including how they were committed and the results of such crimes (what criminals are stealing during vehicle break-ins or home burglaries). Information regarding reoccurring home invasions for example, can be pushed to communities and include helpful information to advise residents on how to better protect their homes during hours of darkness. This also helps police departments develop relationships with residents in an effort to increase two-way information sharing and increase reporting. Law enforcement should consider this an added bonus to the already established benefit of monitoring social media for community threats that are occurring within their area of operation (AO).

SLTLE agencies and their application or use of SOCMINT differs greatly from how federal agencies within the IC are able to use intelligence for national security purposes. Because of this, there are several important aspects of laws and regulations that affect SOCMINT at the SLTLE level, including the associated analysis of the information and how that intelligence is retained by law enforcement agencies. Law enforcement information collection and retention is restricted to statutory laws that fall under the jurisdiction of the appropriate department that is conducting the intelligence process. As mentioned above, the information

collected by LEI operations is more narrowly restricted to issues concerning actual criminal activity. This differs from what the IC can collect as LEI cannot be concerned with national security matters that occur outside of their jurisdiction. According to Carter (2012),

Virtually all information collected by LEI has constitutional protections that must be accounted for. Conversely, the IC is dealing with information and individuals outside the U.S. and the American criminal justice process is rarely used to accomplish their goals. While the IC certainly has legal restrictions, the same constitutional issues of criminal procedure that apply to LEI on a daily basis are rarely of issue to NSI. (p. 7)

In other words, the IC does not need to worry about constitutional rights when collecting intelligence on non-citizens in foreign countries. This differs greatly from how SLTLE agencies are required to operate when they choose to use social media for intelligence purposes. SLTLE intelligence analysts must ensure any use of or collection and retention of personal information must be based on a criminal predicate. Carter (2009, p. 131) describes this in detail as, “The law enforcement officer must have reliable, fact-based information that reasonably infers that a particularly described intelligence subject has committed, is committing, or is about to commit a crime”. Carter (2012) further explains, “...LEI cannot retain open source information in a criminal intelligence record system that identifies individuals or organizations unless a criminal predicate has been established” (p. 8). The application of this rule needs to be followed through to the end of an inquiry and if a criminal connection is not established with reasonable suspicion, the information and analyzed intelligence needs to be destroyed and made unrecoverable. This principle is potentially the most important aspect of law enforcement intelligence and its application as a policing model. When it comes to social media, and individuals posting personal views, opinions or intents, it is very difficult to differentiate between unpopular (or

different) opinions protected by the first amendment or if the individual is exhibiting precursors to criminal actions. For this reason, it is important for law enforcement to vet and protect information while collecting and retaining personally identifying information (PII). One tool SLTLE has at its disposal resides in executive order (EO) 12333 which governs procedures for federal agencies within the IC. This executive order allows federal agencies to collect information on US persons and disclose that information and intelligence to SLTLE provided it is used in an investigation where reasonable suspicion has been established. According to the United States National Archives (2016), EO 12333 states,

2.3 Collection of Information. Agencies within the Intelligence Community are authorized to collect, retain or disseminate information concerning United States persons only in accordance with procedures established by the head of the agency concerned and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order. Those procedures shall permit collection, retention and dissemination of the following types of information:

- (a) Information that is publicly available or collected with the consent of the person concerned;

As stated above, federal law allows agencies within the IC to collect information via open source resources with few stipulations. The subsequent release of that information to other law enforcement entities is governed by the Privacy Act of 1974. In addition to allowing the information to be released to other agencies, the Act outlines the requirements for the information to be released. The United States Department of Justice (2015) details how 5 U.S.C. § 552a(b)(7) (law enforcement request) regulates the dissemination of information from federal agencies to SLTLE by stating dissemination of the information is permissible,

To another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought.

The combination of these regulations assists federal agencies in their ability to help SLTLE intelligence operations provided that the intelligence is used for a civil or criminal law enforcement activity. Even with this help from federal agencies, LEI program administrators still need to ensure the requirements detailed below are followed regardless of where the information or intelligence originally came from.

Law enforcement officers involved with the collection and analysis of social media sites and SOCMINT, need to be aware of how the Constitution specifically applies to the collection and preservation of the social media collected. The most important points to address are the first and fourth amendments. The first amendment offers United States citizens protections that cover their freedom of speech and their right to peacefully assemble. These amendments apply directly to the use of social media and its application in law enforcement intelligence. Social media is perhaps the most widely used public information medium that allows individuals to express their feelings, beliefs, issues and concerns to many people with little effort and no direct physical involvement. If LEI operations choose to use social media as a collection avenue, they need to ensure they respect this constitutional right of the individuals they are collecting information on at all costs. For example, a LEI analyst discovers on social media that an unpopular group plans to have a rally within their city limits. The event might be unpopular, but if there is no reasonable suspicion that a crime has or will take place and the analyst collects personal

information on participating individuals simply because of their unpopular beliefs, they have violated the group's first amendment rights. These protections afforded by the constitution are the very framework that set the United States apart from more oppressive governments. For this reason, LE officers need to ensure they are abiding by these rules and allowing citizens to freely but peacefully express even their unpopular views.

The second important amended that concerns LEI and the use of social media is the fourth amendment. It is very important that the fourth amendment be considered when pulling information from social media sites and conducting SOCMINT operations. Although much of social media is open to the public (open source), many individuals hide or protect their social media lives with the use of privacy settings. However, LEI operations have ways around the privacy settings but need to understand how the collection will be reviewed in court. In 2012 a decision was made in federal court involving the use of Facebook "friends" that allowed federal investigators to access information on accused gangster Melvin Colon (Brunty, 2013). Colon and his attorney's argued that his fourth amendment rights had been violated through the use of Facebook where federal investigators had gained access to Colon's page through an informant who was Facebook friends with Colon. However, Federal Judge William Pauley ruled that Mr. Colon was not protected under the fourth amendment in this case. Brunty (2013), documents Mr. Colons case as follows,

Agents found that Colon had used Facebook to post about violent acts and threats to rival gangs and gang members (Roberts, 2012a). Authorities used such information to obtain a search warrant to investigate the remaining portions of Colon's Facebook account. In his issued opinion, Judge Pauley stated:

Where Facebook privacy settings allow viewership of postings by “friends” the Government may access them through a cooperating witness who is a “friend” without violating the fourth amendment. (p. 71-87)

Cases like this have set precedence and indicate that what an individual might believe is private information, if it is shared with “friends” through social media, it does not qualify as private user information. This creates a grey area that police intelligence teams need to respectfully work through. The goal, as with any police action, is to protect individuals within society while catching the criminals that threaten the peace. These efforts, although difficult, need to respect the rights of even the criminals law enforcement is trying to catch. Without these protections being afforded to citizens, whole groups of societies might begin to not trust their law enforcement officials.

Another important aspect of using social media for information collection and ultimately intelligence analysis is the application of Criminal Intelligence Systems Operating Policies also known as 28 CFR (Code of Federal Regulations) part 23. 28 CFR part 23 may be the most impactful guideline available to LEI analysts. This CFR does not require mandatory adherence to the policy by self-governed state and local police departments who operate under their own authority. It provides more of a recognized policy standard that law enforcement intelligence operations can follow at their discretion. It also extends the protections afforded to individuals to organizations and advises a 5-year review and elimination of intelligence records where no reasonable suspicion of criminal action has been established (Carter, 2009, p. 154). Even though 28 CFR par 23 does not require adherence, law enforcement agencies must follow the regulation requirements to be eligible to receive federal funding to use towards an intelligence program. Thus, there is possibly a substantial financial benefit to adhering to the policy in addition to the

civil lawsuit protections this policy provides to law enforcement departments. The financial benefit alone relieves some of the financial burden for any small police department that relies on additional funding from the federal government to implement policies such as an intelligence program. To add to the impact that 28 CFR part 23 has on intelligence programs across the country, the National Criminal Intelligence Sharing Plan (NCISP) recommended that all police departments adapt 28 CFR part 23 and with this endorsement, 28 CFR part 23 became recognized as the national standard (Carter, 2009).

One issue that 28 CFR part 23 does not address is how to handle an incident where information regarding an individual is reported by the public, but there appears to be no criminal predicate at the time the report is submitted to police. These scenarios cannot be simply dismissed once brought to an officer's attention. To account for this type of situation, an interpretation of 28 CFR part 23 was created in the Law Enforcement Intelligence Unit (LEIU) File Guidelines that allows for two different types of intelligence files (Carter, 2009, p. 154). The LEIU File Guidelines are a "real world" clarification of 28 CFR part 23 and allow for temporary and permanent files to be created and kept separately by intelligence teams. Temporary files are used when situations arise similar to the one mentioned above. These files do not meet the reasonable suspicion criteria but have direct indications related to a possible crime. Public tips or suspicious incident reports would fall into this category. These types of files cannot and should not be considered intelligence and need to be labeled appropriately as temporary files or suspicious incident reports. In essence, these reports or files are only raw information with no application of intelligence analysis being applied. To avoid any privacy rights issues, these files should have a departmental policy clearly defining an expiration date and after an initial inquiry, if no criminal predicate is found, they should be destroyed. If after an

initial review or inquiry, a criminal predicate is discovered that reaches to the level of reasonable suspicion, the file should be transitioned to a permanent file and the regulations of LEI processing that have been discussed here should be applied.

Undoubtedly, there will be incidents where an individual's rights appear to have been violated. Fortunately, citizens have protections and opportunities available to remedy violations of constitutional protections, situations where civil rights were abused or circumstances where privacy was not respected under the law. Title 42 of the United States Code (USC), Section 1983 – Civil Action for Deprivation of Civil Rights allows citizens to seek civil reparations for instances where rights were not protected or respected appropriately. Also known as Section 1983, this USC allows individuals to file civil litigation at the federal court level against individuals acting as law enforcement under government authority. Section 1983 was instituted as part of the Civil Rights Act of 1871 and was originally intended to prevent oppressive behavior by individuals both inside and outside of government (Carter, 2009, p. 156). Section 1983 seeks to establish if the individual's constitutional rights were violated, was state law followed and was the LE agency involved following appropriate policies to ensure an individual's rights were protected. In order to argue a successful civil rights case under Section 1983, a plaintiff must show the LE agency was negligent and that there has been a historical pattern of misconduct that led to the negligence (Carter, 2009, p. 156).

While discussing the use of LEI and how it can use social media to advance its information gathering process, it is important to remember the historic abuses of information collection and privacy violations that have taken place. These historic examples offer opportunities for current and future law enforcement intelligence operations to learn and adapt to stay within the confines of the Constitution and other regulations. During the 1950s, information

was collected and retained with little or no evidence constituting reasonable suspicion. This was propagated by U.S. Senator Joseph McCarthy of Wisconsin. By most accounts, Senator McCarthy waged a relentless hunt for potential communists throughout the United States during his tenure in the Senate. During these years, McCarthy and his team violated numerous civil rights and privacy laws. The law enforcement community needs to stand against any potential repeat of these violations especially with the ongoing threat of Islamic Extremists (IE) and the threat of terrorism. Law enforcement officers are all too often willing to skirt the line between privacy rights violations and catching the criminal. While this type of behavior is noble at its core (wanting to catch a criminal), these are the overreaches that lead to serious abuses of power. It is a very difficult moral situation to be in. On one hand, the criminal might get away and the media will criticize the department and the officers for the lack of prosecution. On the other hand, the criminal's rights might be violated. In this instance, the media and civil rights organizations will lambast the department for any legitimate or even perceived violations. It cannot be forgotten that law enforcement officers have a sworn duty to uphold the laws and protect the rights of citizens no matter what. Even the rights of the worst criminals and violent extremists. These themes need to be at the center of the law enforcement officer's decision making process, not only to protect them from civil litigation, but to also protect the intelligence process and the reputation of LEI operations across the country. Society and the United States citizenry have no tolerance for violations of civil and privacy rights today. The news media perpetuates stories of these violations and often leaves out critical information regarding details of arrests and actual facts of the case. These half stories coupled with the urge to rush to judgement have had serious consequences. This can be seen recently with several police involved shootings that have resulted in violent protests and even the murderous targeting of

police officers in Dallas, Texas. As a best practice, it is important for all LEI programs to adapt and maintain the national standards that have been established to respect the rights of citizens while still allowing the intelligence process to work towards its goal. This not only protects the integrity of LEI programs throughout the nation, but protects agencies and officers from civil liability.

When using social media within an intelligence program, all of these factors contribute to the perception and legitimacy of the intelligence program not only locally, but throughout the country. This is important to remember due to the immediate and far reaching exchange of information that takes place every day as a result of the 24-hour national news cycle. If an intelligence program on the east coast is determined to be unconstitutional or found to be abusing power, civil rights organizations and local residence of departments on the west coast will undoubtedly begin to question their local departments and inquire as to the legitimacy of their intelligence programs. Regardless of whether perceived violations of civil liberties took place or not, police agencies need to ensure they have a transparent process to address the concerns of the public. If the public feels a program is abusing the rights of its citizens, the program will not be able to contribute all available resources to the program and the benefits of the intelligence program will be limited if not lost completely. It is the executive leadership's responsibility to ensure and oversee that nationally recognized standards are being met as a measure of "best practice" to ensure constitutional protections and civil liberties are protect. A core principle of this should include 28 CFR part 23, even if the department is not receiving federal funds to support the program. At the very least, this should be done to promote a sense of transparency to the public the department is serving. As with any developing program, the use of SOCMINT is a developing strategy that is constantly under review. As technology advances and mobile

applications continue to be refined and created, the onus of keeping current with the technologies and the regulations that apply to them, will reside with the intelligence program team.

References

1. Omand, D., Bartlett, J. & Miller, C. (2012). #Intelligence. Retrieved October 23, 2016 from http://www.demos.co.uk/files/_Intelligence_-_web.pdf?1335197327
2. LexisNexis. (2014). Social Media Use in Law Enforcement. Retrieved October 23, 2016, from <https://www.lexisnexis.com/risk/downloads/whitepaper/2014-social-media-use-in-law-enforcement.pdf>
3. Berman, M., Larimer, S., & Wootson, C., Jr. (2016, October 15). Three Kansas men calling themselves ‘Crusaders’ charged in terror plot targeting Muslim immigrants. Retrieved October 23, 2016, from https://www.washingtonpost.com/news/post-nation/wp/2016/10/14/three-kansas-men-calling-themselves-crusaders-charged-in-terror-plot-targeting-muslim-immigrants/?utm_term=.2545e57a3b80
4. Facebook. (n.d.). Company Info | Facebook Newsroom. Retrieved October 23, 2016, from <http://newsroom.fb.com/Company-Info/>
5. Snap Trends Software Features. (n.d.). Retrieved October 23, 2016, from <http://snaptrends.com/social-media-software/features/>
6. Spoto, C. (2014, August 31). Police seeking software for monitoring social media ... Retrieved October 23, 2016, from http://journaltimes.com/news/local/police-seeking-software-for-monitoring-social-media/article_d55bb4f5-4557-5356-bb65-12fc4b4a5ac9.html

7. Carter, D. (2012, November). Law Enforcement Intelligence and National Security Intelligence: Exploring the Differences. *IALEIA Journal*, 21(1). Retrieved October 23, 2016.
8. Signal. (n.d.). Retrieved October 23, 2016, from <http://www.getsignal.info/>
9. Carter, D. L. (2009). *Law enforcement intelligence: A guide for state, local, and tribal law enforcement agencies* (2nd ed.). Washington, DC: U.S. Dept. of Justice, Office of Community Oriented Policing Services.
10. US National Archives. (n.d.). Executive Order (EO) 12333--United States Intelligence activities. Retrieved October 23, 2016, from <https://www.ise.gov/executive-order-eo-12333-united-states-intelligence-activities>
11. US Department of Justice. (2015). Overview of the Privacy Act of 1974. Retrieved October 23, 2016, from <https://www.justice.gov/opcl/conditions-disclosure-third-parties#law>
12. Brunty, J., Helenek, K., & Miller, L. (2013). *Social media investigation for law enforcement*. Abingdon, Oxon: Anderson Pub.