Presented to the Interdisciplinary Studies Program:

UNIVERSITY OF OREGON
APPLIED INFORMATION MANAGEMENT

Applied Information Management
and the Graduate School of the
University of Oregon
in partial fulfillment of the
requirement for the degree of
Master of Science

Law Enforcement Use of Social Media as a Crime Fighting Tool

CAPSTONE REPORT

Kevin Richard Jones
University of Oregon

University of Oregon
Applied Information
Management
Program

Spring 2017

Academic Extension
1277 University of Oregon
Eugene, OR 97403-1277
(800) 824-2714

Approved by

_____

Dr. Kara McFall
Director, AIM Program

Law Enforcement Use of Social Media as a Crime Fighting Tool

Kevin Richard Jones

University of Oregon

Abstract

The increased popularity of social media websites within the last decade has opened a new avenue for law enforcement to access intelligence from criminals who utilize these sites. Law enforcement agencies need to recognize the collection possibilities and understand the various ways that investigators can access this content to progress cases. This annotated bibliography, intended for law enforcement managers, presents best practices and tools in the use of social media as a crime fighting tool.

Keywords: social media, law enforcement, investigations, evidence collection

Table of Contents

Introduction to the Annotated Bibliography 4

Problem Statement 4

Purpose 6

Research Question 6

Audience 7

Search Report 7

Documentation Method 9

Reference Evaluation 9

Annotated Bibliography 11

Rise of Social Media as a Crime Fighting Tool 11

Best Practices in the Use of Social Media as a Crime Fighting Tool 16

Best Practices in Technology that Enable Social Media Use as a Crime Fighting Tool 19

Conclusion 27

The Rise of Social Media as a Crime Fighting Tool 27

Best Practices in the use of Social Media as a Crime Fighting Tool 29

Best Practices in Technology that Enable Social Media Use as a Crime Fighting Tool 29

Summary 31

References 32

Introduction to the Annotated Bibliography

Problem Statement

The Federal Bureau of Investigation (FBI) has a longstanding history of using outdated technology that has a direct impact on the ability to conduct federal investigations (Ryan, 2014). The FBI did not adopt a functioning automated case management system that allowed the maintenance of digital documents until 2012. Prior to this point, the FBI was using the same paper file system that it had used since the creation of the Bureau back in the 1930s (Ryan, 2014). As technology advances, federal investigators can locate criminals and bring their misdeeds to justice if they have access to the technology that is on par with, or ahead of, the criminals they pursue (FBI, 2016). One of the many areas that is a rich source of investigative information are the publicly available data housed on social media sites (Hua, 2015).

The popularity of social media has grown to the point where nearly two-thirds (65%) of all adults in the United States use the websites (Perrin, 2015). Though it may not be seen by the general public, many criminals, even terrorists, use social media accounts for a variety of purposes (Klausen, 2015). Terrorists, for example, use social media to inspire their followers to pick up arms and join their causes, and this information provides significant information to investigators who use it in their investigations (Klausen, 2015). Another way that investigators use social media to collect information is when investigating gangs. Gangs, much like terrorists, use social media to connect with people and to promote their groups to the world (Hua, 2015). If deemed necessary to do so, law enforcement officers can create undercover identities and connect directly with individuals of interest in an effort to access their inner network and gather even more information (*U.S. v. Robison*, 2012). With the use of technology by those breaking the

law, federal investigators need to be able to access these sites to gather information that provides insight and information to assist in arrests and prosecution (FBI, 2016).

A recent study revealed that "eight out of every 10 law enforcement professionals (81%) actively use social media as a tool in investigations" (LexisNexis Risk Solutions, 2014, p. 2). With law enforcement rushing online to look for ways to collect data that may assist it in investigations, there is an obvious need for technology that will allow access to these social media sites housed both on the internet and in applications (ISIL Online, 2016). "Criminals have started to use technology tools when committing crimes. With advanced software and hardware forms of technology, they can commit crimes readily, and crimes have now shifted from their previous more observable methods of operation to the digital realm" (Faith & Bekir, 2015, p. 286). Though the use of the internet to commit crimes today may be more advanced than ever before, it is expected to continue to grow and advance in complexity as criminals become even more sophisticated (International Cyber Security Protection Alliance, n.d).

Former FBI director James Comey stated that his focus is to "…ensure our personnel possess the best possible training, technology, and infrastructure needed to carry out their jobs every day" when he testified before the House Appropriations Committee about the FY 2017 budget (FBI Budget Request, 2016, p. 1). The FBI requested and received approval for $38.3 million related to operational technology investments (FBI Budget Request, 2016). These funds are designated for the support of the FBI in utilizing technology, ensuring that federal investigations are performed using the necessary tools to locate pertinent information (FBI Budget Request, 2016). A part of the overall need for technology within the FBI is related to the need of investigators to access social media sites (ISIL Online, 2016). The funds needed to purchase the technology for accessing these social media sites are present, but the FBI's

acquisition of technology continues to lag and, at times, leaves law enforcement incapable of conducting complete and thorough investigations (FBI, 2017).

Accessing social platforms that criminals use is critical to collecting information that will assist law enforcement agents in successfully working their cases and investigations (ISIL Online, 2016). In order to access social media sites, investigators need access to technology and training to ensure they have the capabilities to leverage what has become a valuable source of information in the fight against crime (ISIL Online, 2016).

Purpose

Crime is still a part of today's digital environment, where social media is now used as a tool for criminals enabling them to commit illegal acts (Hua, 2015). Since the inception of the online internet crime reporting platform in the year 2000, the FBI has received nearly 4 million complaints of internet related crimes including crimes facilitated by social media platforms (Internet Crime Complaint Center, 2015). The purpose of this annotated bibliography is to explore the current gaps in technology and capabilities that prevent law enforcement agents from accessing social media sites to aid in crime fighting. Literature is presented that addresses the growth in the use of social media by criminals and the various ways that criminals are using these platforms. Sources that present best practices and tools in the use of social media as crime fighting tools are highlighted.

Research Question

Question. What are best practices and tools that law enforcement agencies can leverage to use data generated by social media to solve crime?

Audience

The audience for this study is executive management level supervisors within law enforcement agencies. Within the FBI, executive management includes the special agent in charge (SAC), assistant special agent in charge (ASAC), administrative officer (AO), and supervisory intelligence analysts (SIAs), as well as the supervisory information technology specialists (SITSs). These positions constitute the highest level of management within the FBI (FBI Portland Management, 2017) for the state of Oregon and are responsible for all federal investigations, as well as the technology that is used to conduct these investigations. As the highest level of FBI management in Oregon and ultimately responsible for the technology that investigators are using, executive management will likely appreciate that better technology will result in a more effective law enforcement organization overall.

Search Report

Search strategy. In an effort to collect relevant and accurate information related to the use of social media by criminals and barriers to law enforcement access to the data generated by criminals' social media use, a variety of databases were accessed and search strategies implemented. This collection effort was conducted utilizing several databases to access various peer reviewed journals related to criminal law, technology, social media, applications, law enforcement, and investigative techniques. Due to ever-changing technology and the constant developments of apps and social media, the search scope was narrowed to the last five years.

Overall, finding materials contained within the University of Oregon Libraries' site was challenging, as many of the keywords used are related to a very specific type of investigative method and do not seem to be regularly covered within academia. However, some success was

realized using Google Scholar to search research information, which provided a variety of journals and relevant data and statistics.

Key terms. To collect relevant and reliable material, the following key terms, in various combinations, were used:

- Social media,
- Social networks,
- App store,
- Application,
- Criminal justice,
- Federal investigation,
- Open source intelligence (OSINT),
- Criminal research,
- Law enforcement intelligence, and
- Social media law.

Exploration engines and databases. Materials were collected from a variety of peer reviewed academic sources that have direct connections to the related topic of law enforcement's use of social media to conduct investigations. Since there are many topics that can be explored when collecting supporting material, the results of this research were evaluated to ensure that only the most relevant content was included. The use of search engines included Google Scholar and the UO Libraries. The main database queried was JSTOR, an online free database with access to "…more than 10 million academic journal articles, books and primary sources in 75 disciplines" (JSTOR, 2017, p. 1).

Documentation Method

Documentation approach. References were saved in both a Google Sheets document as well as a working Microsoft Word draft that housed the overall project. Storing the references in two separate places provided the necessary backup needed to ensure that the material would not be lost should the main Microsoft Word document fail. Storing the references on a Google Sheets document, which functions just like a Microsoft Excel document, meant the material was stored on the Cloud linked to a Google Gmail account, which could be accessed from anywhere. Storing the references in the Cloud assured that the information was kept safe, yet accessible. The main working copy, a Microsoft Word document, was stored on a USB drive.

The references included in the working document were cited according to American Psychological Association (APA) guidelines. Links to documents were either drafted into APA format manually, or were formatted by utilizing the APA online citation application, Citation Machine. This website was used to help maintain a running list of all citations.

Reference Evaluation

Reference evaluation criteria. To evaluate the credibility of the references, each potential source underwent a variety of reviews before it was included as a supporting document. Potential sources were screened using five criteria to analyze their authority, timeliness, quality, relevancy, and bias (Center for Public Issues Education, n.d.). Authority of a source was determined by noting whether it was authored by professionals with the necessary credentials to write knowledgeably on the topic with sufficient authority to support their claims. The references were filtered for bias by ensuring that the authors had considered alternate perspectives, determining if the author was attempting to sell products or services related to the topic, and ensuring that their conclusions were supported by credible sources. Information sources were

also filtered for quality by checking the punctuation, spelling, and grammar of the material. Information was sought and included only if the information was relevant to the overall topic of this annotated bibliography. To ensure the timeliness of the references, only items published within the last five years were included to reflect the fact that social media is a relatively new development. Older material was included as background when it detailed the history of the FBI (Center for Public Issues Education, n.d.).

Annotated Bibliography

The following bibliography is comprised of 15 references that provide insight into the ways that law enforcement can utilize social media websites as a useful intelligence collection platform as it relates to criminal investigations. References fall into three categories: (a) rise of social media as a crime fighting tool, (b) best practices in the use of social media as a crime fighting tool, and (c) best practices in technology that enable social media use as a crime fighting tool. Some of the references located fall into more than one of the aforementioned categories but were placed in the most logical section. Each reference includes the full citation in APA format, an abstract, and a summary of the content of the publication and a declaration of how it is relevant to the overall study.

Rise of Social Media as a Crime Fighting Tool

Boone, J., & Nagy, S. (2013). *Criminal use of social media* [White paper]. Retrieved from National White Collar Crime Center website: https://www.nw3c.org/docs/research/criminal-use-of-social-media.pdf?sfvrsn=6

Abstract. The authors discuss in detail the specifics of criminal use of social media to communicate, cause, and promote crimes online. The authors also provide the associated statistics of the user base for various social sites, as well as the ways in which the sites are being used by criminals. The authors note the most common online crimes committed, including burglary, phishing, malware, identity theft, and cyberstalking. [Abstract written by the author of this annotated bibliography.]

Summary. In this article published by the National White Collar Center, a variety of crimes are detailed and insight is provided into how they are all affected by the rise in social media popularity within the United States. The article shows how criminals use social media to

communicate with others, how they can commit crimes online, and how they use the information that victims post online to their advantage. This article is relevant to this study as it shows the adaptability criminals have demonstrated by collecting publicly available information provided by social media users and using it when committing crimes. Understanding how criminals are using social media guides law enforcement officials in determining what they need to do to inform the general public of ways to stay safe online.

FBI. (2017, March 17). *Going dark*. Retrieved from https://www.fbi.gov/services/operational-technology/going-dark

Abstract: The issue that law enforcement faces in today's society is the fact that criminals are now *going dark* and are using technology that is incapable of providing subscriber content to law enforcement when provided with a legal order. An example of going dark is someone logging onto the internet using an IP address anonymizer, such as a TOR browser, which restricts an investigator's ability to serve a legal order to a company to determine who accessed the internet and committed a crime. This provides a unique issue for the FBI as it directly impacts its capabilities to complete investigations. [Abstract written by the author of this annotated bibliography.]

Summary. Going dark is a term coined by the FBI in the past several years to explain to lawmakers and the general public about the ways in which criminals are using new technology to conduct illegal activities and avoid the detection of law enforcement agencies. Examples include hackers using technology like TOR browsers to anonymize and disguise their illegal activities online. This report, published by the FBI, explains the ways criminals, including terrorists, are using technology to network and what the FBI and its sister agencies are and are not capable of doing to collect that information when it has the lawful authority to do so. This report is relevant

to this study as it provides current examples of the negative implications on investigations when law enforcement officers cannot access information when technology or policies restrict their access.

Hua, V. (2015, November 11). Law enforcement's growing use of social media to target gang activity (City Square article). *Fordham Urban Law Journal*. Retrieved from http://urbanlawjournal.com/social-media-and-anti-gang-law-enforcement/

Abstract. This article describes various potential uses of social media by law enforcement to target criminal activity, focusing on gang activity and networks. The content details how investigators can glean otherwise difficult to obtain data from these social media pages. The author notes that information such as friendships, familial relations, interests and current locations can all be collected by viewing social media pages. [Abstract written by the author of this annotated bibliography.]

Summary. In the article published in the Fordam Urban Law Journal, author Vinh Hua discusses the increasing amount of time that people are spending online and how criminals, especially those in gangs, are also using these sites. Hua believes that in pursuing the adoration of their peers, these gang members post pictures and status updates of themselves that may actually incriminate them in criminal cases. Hua dives into how the police can then access these websites and gather information that can lead to convictions and prosecutions of criminals and provide justice for crime victims. He details how police can create fake social accounts that are used to access previously blocked content. This article is relevant for this study as it provides information about why criminals choose to post incriminating information on their social media profiles and the many ways that law enforcement can access this information to aid in investigations.

Internet Crime Complaint Center. (2015). *2015 Internet crime report*. Retrieved from https://pdf.ic3.gov/2015_IC3Report.pdf

Abstract: The Internet Crime Complaint Center, which is managed by the FBI, is the main funnel for all internet related crimes, including crimes linked to social media, that individuals wish to report to the FBI. The 2015 report details the various types of crimes reported as well as the various details associated with the reports such as the type of crime, total loss amount, and location in which the crime happened. [Abstract written by the author of this annotated bibliography.]

Summary. The Internet Crime Complaint Center creates a report at the end of each year that provides a significant amount of detail into the many ways that criminals are using the internet to facilitate their crimes. The report provides statistics into the various types of crimes that have been reported since the inception of the program, which is already nearing its four millionth internet crime report provided to the center. These crime reports are provided to the center by public and private entities. The center's annual report details age ranges, sex, and locations that have been most affected by the crimes reported. In 2015 alone, victims lost an estimated $55 million to criminals who were committing crimes by utilizing the internet to some extent. This report is relevant to this study as it provides detailed victim information related to online crimes, including crimes related to social media.

ISIL online: Countering terrorist radicalization and recruitment on the Internet and social media. Statement before the Permanent Subcommittee on Investigations of the Senate Committee on Homeland Security and Governmental Affairs, 114th Cong., Second Session (2016) (testimony of Michael Steinbach). Retrieved from

https://www.fbi.gov/news/testimony/isil-online-countering-terrorist-radicalization-and-recruitment-on-the-internet-and-social-media-

Abstract. This statement by Michael Steinbach, FBI Executive Assistant Director of the National Security Branch, details the threat to national security if terrorists use technology that law enforcement cannot access and continue to recruit using social media platforms. Assistant Director Steinbach notes that many digital platforms used by terrorists are making the job of law enforcement even more difficult. One example is Tor browsers, which criminals and terrorists can use to disguise online activities because TOR browsers scramble IP addresses, making it essentially impossible for law enforcement to locate the individual responsible for the online activity, especially as it pertains to social media activity. [Abstract written by the author of this annotated bibliography.]

Summary. In a statement provided to the Senate Committee on Homeland Security and Government Affairs, FBI Executive Assistant Director Steinbach discusses how social media platforms and other digital technology are no longer being used just by everyday citizens, but are now being used as a recruitment platform by terrorist organizations overseas to connect with and inspire individuals within the United States. When these groups publish terrorist propaganda online, it is often marketed towards westerners whom they are hoping will view the content and be willing to commit terrorist activities on behalf of these organizations. This provides a unique issue for law enforcement agencies as they face a difficult time trying to determine who is receiving these messages and if those people are taking steps towards planning an act of terrorism. Specific challenges include determining who is responsible for posting terrorist recruitment propaganda online, who is accessing this material, what they are planning to do with this information, and what law enforcement can do to get ahead of it to prevent the action.

This report is relevant for this study as it shows that social media is being used by a wide variety of criminal organizations, including terrorist organizations. Accessing social media platforms to follow the activities of these organizations is critical if national security agencies hope to prevent future terrorist events, but success in these efforts has been hindered by the inaccessibility of some of these sites to law enforcement due to limited technology in some field offices. The report provides a summary of issues faced by law enforcement agencies in leveraging social media to thwart terrorist activities.

Best Practices in the Use of Social Media as a Crime Fighting Tool

Faith, T., & Bekir, C. (2015, April). Police use of technology to fight against crime. *European Scientific Journal, 11*(10), 286-296. Retrieved from http://eujournal.org/index.php/esj/article/download/5426/5322

Abstract. Traditionally, law enforcement agencies have had an unfriendly relationship with technology. However, there is no way one can ignore and/or resist the adoption of new technologies any longer since recent developments in information technology have changed the attitudes and perceptions of police forces as well as criminals. The technological advances over the years have provided law enforcement agencies new perspectives and considerations beyond the traditional methods and opportunities to utilize a wide range of innovations in different contexts. The recent innovations and implementations which increase the efficiency and effectiveness of policing including network analysis, GIS, crime mapping, biometrics, fingerprints, DNA research, facial recognition, speech recognition, social media policing, shotspotter detection system, and CCTV are detailed in this study.

Summary. Faith and Bekir (2015) discuss the ways that law enforcement worked with technology in the past and note that they have not always been successful in obtaining and

working with the latest technology. The authors detail how the rise in technology over the past several years has encouraged law enforcement agencies to leverage technology more successfully when fighting crime. Technological innovation has provided law enforcement agencies with useful tools such as facial recognition, speech recognition, crime mapping, biometrics, network analysis, and social media policing. This article is relevant to this study because it shows how law enforcement agencies have been traditionally slow to adopt technology as it becomes available, but are now using a variety of specific technologies and tools to fight crime.

Murphy, J. P., & Fontecilla, A. (2013, April). Social media evidence in government investigations and criminal proceedings: A frontier of new legal issues. *Richmond Journal of Law & Technology, XIX*(3). Retrieved from http://jolt.richmond.edu/2013/04/03/social-media-evidence-in-government-investigations-and-criminal-proceedings-a-frontier-of-new-legal-issues/

Abstract. As the newest pillar of communication in today's society, social media is revolutionizing how the world does business, discovers and shares news, and instantly engages with friends and family. Not surprisingly, because social media factors into the majority of cases in some respect, this exploding medium significantly affects government investigations and criminal litigation. Social media evidence includes, among other things, photographs, status updates, a person's location at a certain time, and direct communications to or from a defendant's social media account. This article will examine the importance of social media in government investigations and criminal litigation, including access to and use of social media evidence, constitutional issues that social media evidence raises, the authentication and admissibility of such evidence, in addition to the impact of social media on jurors.

Summary. In this article published in 2013 by the *Richmond Journal of Law and Technology*, Murphy and Fontecilla take a unique approach to the increased use of social media and discuss legal issues that may arise for law enforcement when accessing information from online social media websites. They list legal issues that need to be considered before locating, storing, and providing material to use during prosecution. The authors describe the ways in which social media companies react to subpoenas and warrants, the Stored Communications Act, Constitutional rights as they pertain to social media evidence, admissibility of such evidence, and how this type of evidence is commonly viewed by juries. This article is relevant to this study due to its coverage of the legal aspects related to the collection of social media evidence and its recommendation that law enforcement agencies should consider the legal implications before collecting such information.

Rice, S. K., & Parkin, W. S. (2016, December). *Social media and law enforcement investigations* (Oxford handbooks online scholarly research review). doi: 10.1093/oxfordhb/9780199935383.013.98

Abstract. The use of social media applications and services have become ubiquitous in the United States, even more so among teenagers and young adults within their prime offending years. At the same time, law enforcement agencies have been challenged to keep abreast of these technological changes, both from a procedural and legal perspective. This article outlines the use of social media in law enforcement investigations, focusing specifically on investigations regarding "routine" crimes, counter-terrorism or extremism, police use of force, and misconduct allegations. Although the empirical research in this area is severely limited, we present current agency practices and examples for "routine," internal, and ideological investigations. We

conclude with suggestions for future research agendas that can provide more insight and understanding into law enforcement's use of social media as an investigatory tool.

Summary. In this article, Rice and Parkin (2016) discuss how social media has been increasing in popularity and the fact that criminals are choosing to use these platforms during their prime offending years. They discuss how members of law enforcement are slowly adapting to this increase in technology and are beginning to use it to their advantage as an investigative tool. Rice and Parkin discuss how to use social media for routine criminal investigations, including researching criminal networks and determining current locations of individuals. The authors also provide recommendations for how to exploit social media for terrorism investigations, including identifying terrorist networks and levels of radicalization. Finally, Rice and Parkin recommend ways to use social media as a form of law enforcement accountability, including increasing transparency regarding police activities and connecting on a more personal level with the surrounding community. This article is relevant to this study as it shows how law enforcement agencies are using social media platforms as crime fighting tools for various types of offenses.

Best Practices in Technology that Enable Social Media Use as a Crime Fighting Tool

Perrin, A. (2015, October 8). Social media usage: 2005-2015. Retrieved from the Pew Research Center website: http://www.pewinternet.org/2015/10/08/2015/Social-Networking-Usage-2005-2015/

Abstract. Nearly two-thirds of American adults (65%) use social networking sites, up from 7% when Pew Research Center began systematically tracking social media usage in 2005. Pew Research reports have documented in great detail how the rise of social media has affected such things as work, politics and political deliberation, communications patterns around the

globe, a well as the way people get and share information about health, civic life, news consumption , communities, teenage life, parenting, dating and even peoples level of stress.

Summary. The Pew Research Center published a report revealing how almost 65% of adults in the United States used social media as of 2015. Other statistics include the most common users of social media detailed by age, gender, race, and socioeconomic status. Each of the categories provided by the Pew Research Center can be compared to the statistics from the past ten years to provide a clear example of how much the user bases of social media sites are growing.

This article is relevant to this study as it illustrates how much the use of social media websites have grown in a short period of time and, statistically, the demographics of the people who law enforcement can expect to find using social media accounts. The report also demonstrates the increase in technology advancements over the past decade and the spike in technological capabilities that internet companies now have to serve such a high number of daily users on social media sites.

LexisNexis Risk Solutions. (2014, November). *Social media use in law enforcement: Crime prevention and investigative activities continue to drive usage*. Retrieved from http://www.lexisnexis.com/risk/downloads/whitepaper/2014-social-media-use-in-law-enforcement.pdf

Abstract. Social media is increasingly valuable to the way law enforcement professionals operate in both crime prevention and investigation. However, as social media use becomes more prevalent, there remain many questions regarding how exactly it is utilized to optimal effect in criminal investigations. LexisNexis®, in a follow-up to its initial study in 2012, sought to further examine the law enforcement community's understanding of, and ongoing efforts to leverage

social media. The LexisNexis 2014 Social Media Use in Law Enforcement report looks at current practices and processes and how the landscape has changed over the last two years in addition to new survey research areas.

Summary. LexisNexis authored this article, which details the ways in which law enforcement is rapidly moving towards using social media as an investigative tool. The article provides statistics of how law enforcement agencies are migrating towards using social media platforms and even collecting information provided by social media users; these statistics provide an indication of how these agencies may be using these tools in the future. The report also breaks down the differing attitudes of law enforcement officers towards the usefulness of certain social sites such as Facebook and Twitter. LexisNexis Risk Solutions details the different ways that law enforcement is using these social sites, including researching individuals to aid in active investigations, monitoring special events, using a site to notify the public of crimes, or using a site to notify the public of emergencies or disasters. This article is relevant to this study as it shows how agencies were using social media in the past, provides specific examples of how they are using it now to fight crime, and forecasts how it will be used in the future.

FBI budget request for fiscal year 2017. Hearing before the Subcommittee on Commerce, Justice, Science, and Related Agencies, of the House Appropriations Committee, 114th Cong., Second Session. (2016) (testimony of James B. Comey). Retrieved from https://www.fbi.gov/news/testimony/fbi-budget-request-for-fiscal-year-2017

Abstract. This source provides testimony from former FBI Director, James Comey, during his request for the FY2017 budget for the FBI agency. One element of Director Comey's budget request was funding for technology to be used in the fight against crime. [Abstract written by the author of this annotated bibliography.]

Summary. This testimony given by former FBI Director James Comey to the House Appropriations Committee provides insight into his focus as the leader of the FBI on ways to ensure that the FBI has the necessary technology to succeed in its mission. One specific aspect of technology use as a tool to fight crime that was noted by Comey is the use of technology to access the online sites frequented by criminals. The testimony also provides information about the exact amount of money the organization requests in technology funds, and what the Bureau plans to do with the funds if/when they are approved and allocated. This information is relevant to this study as it provides insight into the leadership priorities of the FBI specifically related to the use of technology to support investigations and the money that the Bureau receives to address these areas.

FBI. (2016, November 1). *A primer on Dark Net marketplaces: What they are and what law enforcement is doing to combat them.* Retrieved from https://www.fbi.gov/news/stories/a-primer-on-darknet-marketplaces

Abstract. This article was released by the FBI and provides details about the DarkNet, a restricted access network used mainly for illegal peer-to-peer file sharing, and how the FBI uses technology to access the content housed within it. It also provides success stories of what the FBI can accomplish when it has access to technology that is on par with the technology that criminals are using. [Abstract written by the author of this annotated bibliography.]

Summary. This article published by the FBI provides information about the DarkNet and the issues that law enforcement faces when trying to locate criminals who utilize these services. The DarkNet is a platform that disguises the online activity of criminals, who have used the platform for a long time for illegal, peer-to-peer file sharing. The FBI discusses how it is able to use available technology to combat these issues and assist its international partners, including

Australia, Canada, New Zealand, and the United Kingdom. Specific practices the FBI noted include the FBI seizing computer servers hosting these websites and identifying the individuals who accessed the sites for illicit means. This article is relevant to this study as it details only some of the advanced technology and social media platforms that criminals are using and the levels of success that law enforcement can reach in fighting these criminals when they have the necessary technology to access them.

Klausen, J. (2015). Tweeting the Jihad: Social media networks of western foreign fighters in Syria and Iraq. *Studies in Conflict & Terrorism, 38*(1), 1-22. http://dx.doi.org/10.1080/1057610X.2014.974948

Abstract. Social media have played an essential role in the jihadists' operational strategy in Syria and Iraq, and beyond. Twitter in particular has been used to drive communications over other social media platforms. Twitter streams from the insurgency may give the illusion of authenticity, as a spontaneous activity of a generation accustomed to using their cell phones for self-publication, but to what extent is access and content controlled? Over a period of three months, from January through March 2014, information was collected from the Twitter accounts of 59 Western-origin fighters known to be in Syria. Using a snowball method, the 59 starter accounts were used to collect data about the most popular accounts in the network-at-large. Social network analysis on the data collated about Twitter users in the Western Syria-based fighters points to the controlling role played by feeder accounts belonging to terrorist organizations in the insurgency zone, and by Europe-based organizational accounts associated with the banned British organization, Al Muhajiroun, and in particular the London-based preacher, Anjem Choudary.

Summary. Jytte Klausen (2015) takes an in-depth look at how social media is being used by terrorists, specifically Western-origin fighters known to be in Syria. Klausen collected and analyzed accounts housed in dozens of different social media platforms and provided results that cover many different categories of effective communication. Categories discussed by Klausen include the past and present ways that terrorists are communicating terror, the ways that ISIS used Twitter in the Spring of 2014, the ways researchers collected data from these accounts, what the terrorists tweet about, how they use pictures as propaganda, and the overall size of the network of these accounts. This article is relevant to this study as it shows how terrorists are using social media and provides insight into ways that law enforcement can replicate the same processes to locate these foreign fighters to effectively provide actionable intelligence to the world's intelligence community.

U.S. v. Robison. (2012, April 2). Case No. 11CR380 (DWF/TNL). United States District Court, D Minnesota. Retrieved from https://www.gpo.gov/fdsys/pkg/USCOURTS-mnd-0_11-cr-00380/pdf/USCOURTS-mnd-0_11-cr-00380-0.pdf

Abstract. This court case provides insight into the capabilities that law enforcement when using undercover identities to communicate with people of interest on social media websites. Also discussed are some of the legal issues that were raised in federal court regarding the legality of law enforcement procedures when creating these undercover accounts. [Abstract written by the author of this annotated bibliography.]

Summary. This court case, United States of America v. Christopher Robison, details how police used undercover social media accounts in real investigations as a crime fighting tool. In short, the Crow Wing County Sheriff's Department created a fictitious profile and communicated with a man looking to have an inappropriate relationship with a young female.

After law enforcement arrested Mr. Robison, it faced legal hurdles in court about the admissibility of some of the material that was collected during the course of the undercover investigation. This article is relevant to this study as it demonstrates the effectiveness of law enforcement agencies in using social media as an investigative tool to communicate with and aid in the capture of criminals who are committing crimes online.

International Cyber Security Protection Alliance. (n.d). *Scenarios for the future of cybercrime*. Retrieved from http://2020.trendmicro.com/Project2020.pdf

Abstract. The ICSPA collected the various types of cyber related crimes, social media included, and analyzed where these crimes are at currency with complexity and popularity and present an outline of what governments, businesses, and individuals can expect these crimes to look like in the future as technology progresses. [Abstract written by the author of this annotated bibliography.]

Summary. The International Cyber Security Protection Alliance (ICSPA) authored this white paper to provide examples of how law enforcement agencies can anticipate today's computer-related crimes to advance in complexity and popularity in the near future. Content includes the types of crimes currently trending and how these may adapt moving forward. Areas of interest include the implications for cybersecurity stakeholders, cybercriminal threats, what the crimes looked like in 2012, and how these crimes will adapt and what they may look like in 2020, and beyond. The white paper recommends that law enforcement agencies need to prepare for cybercrimes to expand to other wireless devices besides computers such as wireless pacemakers and insulin pumps, crimes that are predicted to cause havoc. This white paper is relevant to this study as the material demonstrates how crimes are continually evolving and how

law enforcement will need to evolve as well if it hopes to adapt to the changing technology of tomorrow's social media.

Conclusion

The increased popularity of social media websites within the last decade has opened a new avenue for law enforcement to access intelligence from criminals who utilize these sites (Rice & Parkin, 2016). As technology advances, federal investigators are aided in locating criminals and bringing their misdeeds to justice when they have access to technology that is on par with, or ahead of, the criminals they pursue (FBI, 2016). Social media websites have become a rich source of investigative information due to the amount of publicly available data that is provided by individuals themselves (Hua, 2015). Law enforcement agencies are beginning to recognize the collection possibilities and understand the various ways that investigators can access this content to progress cases (Boone & Nagy, 2013).

The Rise of Social Media as a Crime Fighting Tool

One of the biggest changes in the field of law enforcement investigations has been the increased amount of time that people are spending online and how criminals are using these sites (Boone & Nagy, 2013). Social media is becoming a tool of choice for many criminals (Internet Crime Complaint Center, 2015), and Rice and Parkin (2016) note that criminals are choosing to use social media platforms during their prime offending years. In 2015, crime victims lost an estimated $55 million due to crimes linked to the internet and social media, just in the United States alone (Internet Crime Complaint Center, 2015). Internet and social media crimes include burglary, phishing, malware, identity theft, and cyberstalking (Boone & Nagy, 2013). Hua (2015) noted that criminals choose to use these sites for a variety of reasons, such as gang members who pursue the adoration of their peers by posting photos and status updates, but this online activity also provides law enforcement with the opportunity to access the social sites and collect incriminating evidence.

Because law enforcement has been successful in accessing social media sites and locating individuals who use these sites, some criminals have become more advanced in their tactics to avoid law enforcement and have begun to access the dark web to use social websites (FBI, 2017). The term going dark has been coined to describe the use of technology that is incapable of providing subscriber content to law enforcement when presented with a legal order (FBI, 2017). An example of the dark web is someone logging onto the internet to commit a crime using an IP address anonymizer, like a TOR browser, which restricts an investigator's ability to serve a legal order to a company to determine who accessed the internet and committed the crime (FBI, 2017).

Law enforcement is particularly concerned that conversations on the dark web are happening without law enforcement being able to access the information, especially as it pertains to terrorism investigations and threats against national security (ISIL Online, 2016). When law enforcement agents are successful in accessing social networks on the dark web, the networks provide an immense amount of investigative information to law enforcement agencies, who oftentimes share this data with international partners within the intelligence community (FBI, 2017). Though law enforcement has had success pursuing criminals in the dark web, it is becoming more and more difficult to trace criminal activity when law enforcement officers cannot access information because technology or policies restrict their access (FBI, 2017).

What does the future hold for computer related crimes? Analysts report that crimes being committed on or supported by the internet continue to increase in frequency (International Cyber Security Protection Alliance, n.d). The International Cyber Security Protection Alliance (ICSPA) warned that cybercrimes will likely span to medical devices such as wireless pacemakers and wireless insulin pumps in the near future.

Best Practices in the use of Social Media as a Crime Fighting Tool

A variety of best practices have been developed to access social media websites to collect information and use the data to fight crime (Murphy & Fontecilla, 2013; Rice & Parkin, 2016). Rice and Parkin (2016) identified uses of social media for routine criminal investigations, including researching criminal networks and determining current locations of individuals and exploiting social media for terrorism investigations, including identifying terrorist networks and levels of radicalization. Rice and Parkin also recommend ways to use social media as a form of law enforcement accountability, including increasing transparency regarding police activities and connecting on a more personal level with the surrounding community.

Though there is a plethora of digital information that agencies can collect to aid their cases, Murphy and Fontecilla (2013) noted that law enforcement should understand the limits of the data that internet service providers retain as per the Stored Communications Act, which addresses the compelled and voluntary disclosure of such records. Murphy and Fontecilla also asserted that agencies need to be familiar with the admissibility of social media evidence in court. While law enforcement agencies now routinely use social media sites to gather information on both domestic criminals and terrorists, legal concerns with their associated investigative approaches have been raised (*U.S. v. Robison*, 2012). For example, in the court case of United States of America v. Christopher Robison (2012), legal issues arose in court after undercover investigators gathered evidence by creating a fictitious social media profile to catch a man who was seeking an inappropriate relationship with a young female.

Best Practices in Technology that Enable Social Media Use as a Crime Fighting Tool

According to a 2014 report from Lexis Nexis Risk Solutions, Facebook and Twitter were the most useful social sites in aiding investigations. The Lexis Nexis Risk Solutions report also

noted that law enforcement agencies are not limited to just researching individuals and can use these social websites in a variety of ways, including monitoring special events, using a site to notify the public of crimes, or using a site to notify the public of emergencies or disasters. Faith and Bekir (2015) noted that while law enforcement has not always been successful in obtaining and working with the latest technology, data mined from social media accounts can now be used to assist law enforcement agencies in deploying tools such as facial recognition, speech recognition, crime mapping, biometrics, network analysis, and social media policing.

Although the aforementioned law enforcement uses are commonly deployed as tactics domestically, the increase in social media and the increased presence of internet providers in the Middle East has provided opportunities for international terrorists to communicate their messages to the world (Klausen, 2015). Though there are many negatives associated with this capability, the expansion of social media through increased internet providers in countries that attract terrorist cells and the ensuing use of social media by these terrorists also provides law enforcement with the opportunity to locate these foreign fighters to effectively provide actionable intelligence to the international intelligence community (Klausen, 2015).

Technology has become such a focus in recent years and the increased use of social media as a crime fighting tool has pushed federal agencies like the FBI to request upwards of $38 million related to operational technology investments (FBI, 2017). Some of the funding is allocated to address the ever-changing landscape of the DarkNet, a restricted access network used mainly for illegal peer-to-peer file sharing (FBI, 2016). The FBI has used advanced methods and technology to seize illegal peer-to-peer file sharing social network computer servers, thus enabling agents to locate and arrest the criminals using the DarkNet (FBI, 2016).

Summary

The use of social media sites by the general public continues to rise. The Pew Research Center reported that nearly 65% of adults in the United States used social media as of 2015 (Perrin, 2015). As social media use has risen, criminals also have used social media to communicate, cause, and promote crimes online (Boone & Nagy, 2013). Law enforcement has responded by using social media and associated technology as crime fighting tools (Hua, 2015). In addition to fighting domestic crimes via social media, law enforcement agencies have leveraged the information to fight terrorists (Rice & Parkin, 2016) who use social media as recruitment tools, often via technology that disguises their online activities (ISIL Online, 2016). Law enforcement use of social media has become a critical crime fighting tool that protects communities, counties, states, and the entire United States of America.

References

(Boone, J., & Nagy, S. (2013). *Criminal use of social media* [White paper]. Retrieved from National White Collar Crime Center website: https://www.nw3c.org/docs/research/criminal-use-of-social-media.pdf?sfvrsn=6

Center for Public Issues Education. University of Florida. (n.d.). *Evaluating information sources.* Retrieved from http://ae-coursematerials.uoregon.edu/aim/Capstone1Perm/evaluateinfo.pdf

Faith, T., & Bekir, C. (2015, April). Police use of technology to fight against crime. *European Scientific Journal, 11* (10), 286-296. Retrieved from http://eujournal.org/index.php/esj/article/download/5426/5322

FBI. (2016, November 1). *A primer on Dark Net marketplaces: What they are and what law enforcement is doing to combat them.* Retrieved from https://www.fbi.gov/news/stories/a-primer-on-darknet-marketplaces

FBI. (2017, March 17). *Going dark.* Retrieved from https://www.fbi.gov/services/operational-technology/going-dark

FBI budget request for fiscal year 2017. Hearing before the Subcommittee on Commerce, Justice, Science, and Related Agencies, of the House Appropriations Committee, 114th Cong., Second Session (2016) (testimony of James B. Comey). Retrieved from https://www.fbi.gov/news/testimony/fbi-budget-request-for-fiscal-year-2017

FBI Portland Management. (2017, May 29). *Portland field office.* Retrieved from https://www.fbi.gov/contact-us/field-offices/portland

Hua, V. (2015, November 11). Law enforcement's growing use of social media to target gang activity (City Square article). *Fordham Urban Law Journal*. Retrieved from http://urbanlawjournal.com/social-media-and-anti-gang-law-enforcement/

International Cyber Security Protection Alliance. (n.d). *Scenarios for the future of cybercrime*. Retrieved from http://2020.trendmicro.com/Project2020.pdf

Internet Crime Complaint Center. (2015). *2015 Internet crime report*. Retrieved from https://pdf.ic3.gov/2015_IC3Report.pdf

ISIL online: Countering terrorist radicalization and recruitment on the Internet and social media. Statement before the Permanent Subcommittee on Investigations of the Senate Committee on Homeland Security and Governmental Affairs, 114th Cong., Second Session (2016) (testimony of Michael Steinbach). Retrieved from https://www.fbi.gov/news/testimony/isil-online-countering-terrorist-radicalization-and-recruitment-on-the-internet-and-social-media-

JSTOR. (2017). *About JSTOR*. Retrieved from http://about.jstor.org

Klausen, J. (2015). Tweeting the Jihad: Social media networks of western foreign fighters in Syria and Iraq. *Studies in Conflict & Terrorism, 38*(1), 1-22. http://dx.doi.org/10.1080/1057610X.2014.974948

LexisNexis Risk Solutions. (2014, November). *Social media use in law enforcement: Crime prevention and investigative activities continue to drive usage*. Retrieved from http://www.lexisnexis.com/risk/downloads/whitepaper/2014-social-media-use-in-law-enforcement.pdf

Murphy, J. P., & Fontecilla, A. (2013, April). Social media evidence in government investigations and criminal proceedings: A frontier of new legal issues. *Richmond*

Journal of Law & Technology, XIX(3). Retrieved from http://jolt.richmond.edu/2013/04/03/social-media-evidence-in-government-investigations-and-criminal-proceedings-a-frontier-of-new-legal-issues/

Perrin, A. (2015, October 8). *Social media usage: 2005-2015*. Retrieved from Pew Research Center website: http://www.pewinternet.org/2015/10/08/2015/Social-Networking-Usage-2005-2015/

Rice, S. K., & Parkin, W. S. (2016, December). *Social media and law enforcement investigations* (Oxford handbooks online scholarly research review). doi:10.1093/oxfordhb/9780199935383.013.98

Ryan, M. E. (2014, May 28). *Privacy impact assessment for the SENTINEL System*. Retrieved from https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/sentinel

U.S. v. Robison. (2012, April 2). Case No. 11CR380 (DWF/TNL). United States District Court, D Minnesota. Retrieved from https://www.gpo.gov/fdsys/pkg/USCOURTS-mnd-0_11-cr-00380/pdf/USCOURTS-mnd-0_11-cr-00380-0.pdf