THE EXPLOITATION OF SOCIAL MEDIA BY CLANDESTINE GROUPS, HOW LAW ENFORCEMENT & INTELLIGENCE CAN BETTER UTILIZE SOCIAL MEDIA, AND LEGAL CONCERNS TO ENSURE ITS APPROPRIATE USE BY GOVERNMENT ENTITIES

A Thesis

Presented to the

Faculty of

San Diego State University

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

in

Homeland Security

---

by

Mindy Chidester

Summer 2012

SAN DIEGO STATE UNIVERSITY

The Undersigned Faculty Committee Approves the

Thesis of Mindy Chidester:

The Exploitation of Social Media by Clandestine Groups, How Law Enforcement & Intelligence Can Better Utilize Social Media, and Legal Concerns to Ensure its Appropriate Use by Government Entities

Eric G. Frost, Chair
Graduate Program in Homeland Security

Steven Andres
Graduate Program in Homeland Security

Kevin Robinson
Department of Geological Sciences

George Bressler
Graduate Program in Homeland Security

15 MAY 2012
Approval Date

DEDICATION

I dedicate this work to my dear husband, George, who has patiently supported me during this process. I also would like to dedicate this to my extremely supportive parents and in-laws. I would have never completed this without their help. I also wanted to thank my committee members and their willingness to work with me and more importantly, mentor me.

ABSTRACT OF THE THESIS

The Exploitation of Social Media by Clandestine Groups, How
Law Enforcement & Intelligence Can Better Utilize Social Media,
and Legal Concerns to Ensure its Appropriate Use by Government
Entities
by
Mindy Chidester
Master of Science in Homeland Security
San Diego State University, 2012

Social Media has changed how society communicates and how it views itself. With the world making the massive shift to the sharing of information via online social networks, clandestine groups are exploiting these platforms for their own purposes. There is strong evidence that groups such as Islamic terrorists, white supremacy organizations, and Mexican drug cartels are utilizing these online media sites for communication, recruitment, propaganda, cybercrime, and intelligence gathering. Although law enforcement and intelligence officials have partially recognized the utility of social media in investigations and intelligence gathering, they face tremendous hurdles that prevent more effective application of many social media tools. Among these hurdles, which are giving these groups an enormous advantage are: (1) lack of coordination among agencies, (2) low public trust and cooperation with law enforcement and the intelligence community by many portions of the public, (3) decreased budgets preventing government entities from developing new solutions, (4) rules and policies against the use of social media in government agencies, (5) and unfamiliarity with the functionality and nuances (including jargon and foreign languages) in social media by traditional law enforcement and intelligence community. Nevertheless, there are solutions that may alleviate many of these problems, but only if these solutions are pursued and allowed by the protocols and laws that control law enforcement and intelligence groups. Overall, free to low cost tools can play an extremely large role in assisting law enforcement and the intelligence community.

While social media should become a greater part of many law enforcement investigations and intelligence gathering, government officials must respect and protect citizens' rights and abide by the laws. However they must also be aware that the "bad guys" are using social media in ways that are beyond the law and very much to the disadvantage of law enforcement and other legitimate parts of government and society. Because of the speed of innovation and technology advancement, laws that govern law enforcement and the intelligence community are rapidly becoming ineffective as tools to protect citizens of this country against the schemes of criminal organizations including in arenas of fraud, theft, human trafficking, and dozens of other aspects of the criminal world, Congress and the courts must consider updating current laws to apply to newer technologies in ways that law enforcement and the courts can appropriately prosecute criminals nationally and internationally. Law enforcement and intelligence groups will absolutely have to make

changes in what they are doing as the enormity of the changes in social media have fundamentally changed the world.

TABLE OF CONTENTS

PAGE

LIST OF FIGURES

PAGE

CHAPTER 1

INTRODUCTION

Since the rise of social network sites and their saturated presence in modern culture, various communities of scholars, policy makers, information technology professionals, advertisers, and private-sector companies have studied and weighed the power and importance of these sites. Nevertheless, its nascent presence and constantly changing nature have left much to study. This paper will deal with the application of social media in law enforcement and intelligence gathering when dealing with clandestine and nefarious groups such as Islamic terrorist groups and Mexican drug cartels. In this thesis it will be demonstrated how social network sites can be utilized in monitoring and investigations in an easily accessible and low-cost manner.

Before delving into the specifics of how social media is exploited and how law enforcement and the intelligence community (IC) can exploit the tools of social media, it is of value to discuss the definition of social media and social network sites in order to build context.

In this paper, the term "social media" will be used in the general context of current usage in this Internet society. As the singular form of media, medium connotes the "means for communicating or diffusing information".[1] As such, social media suggests the online social means for communicating and/or diffusing information. In this paper, social media is defined as Internet-based applications that encompass a variety of platforms including, but not limited to social networks, blogs, micro blogs, file-sharing sites, and locative media. This is the definition of the Open-Source Center, which is part of the Office of the Director of National Intelligence (ODNI) and a leading group seeking to use social media for national security. In addition to the ONDI definition of social media, virtual worlds and online gaming are also included in this work as other social media platforms although they are not

[1] "Definition of medium," *Collins World English Dictionary Online*, accessed January 2, 2012, http://www.collinsdictionary.com/dictionary/english/medium.

included in the Open Source Center's classification. As such, the term "social network sites" is just one variety of social media.

In order to avoid unnecessary confusion, no distinction will be made between social network sites and social networking sites; both will simply be referred to primarily with the term "social network sites" (SNS). In contrast, Danah Boyd and Nicole Ellison have distinguished the two terms as the former being used as a means to communicate with people who are already a part of their existing and extended social network, whereas, the latter implies its purpose is for meeting and networking with others.[2] Though they make a valid point, the purposes and uses of modern social network sites have blurred; people often connect with those they know from school or work, but may also connect with those who have common friends or interests. Rarely are SNS used only for one or the other now. As such, social networking sites and social network sites will be considered the same and can be used interchangeably.

To better explain what social media does and is, several examples of the different platforms will hopefully clarify this dialogue. As mentioned, the DNI Open Source Center categorizes social media into varying platforms.[3] It is prudent to note that these platforms are not mutually exclusive that many platforms combine functions or have similar functions to other platforms.

Social network sites are one of the most discussed forms of social media. Boyd and Ellison defined SNS as:

> Web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.[4]

More generally speaking, social network sites are also defined as an online platform or site that focuses on building and reflecting existing relationships or networks among people and

[2] Danah M. Boyd and Nicole B. Ellison, "Social Network Sites: Definition, History, and Scholarship," *Journal of Computer-Mediated Communication* 13: 210–230, http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2007.00393.x/full.

[3] "Social Media for Intelligence Professionals," *Drug Enforcement Administration*, (Handout from DNI Open Source Center, San Diego, CA, January 25, 2012.)

[4] Boyd and Ellison, "Social Network Sites…"

organizations. Social networks have additional functions as they allow the average person to share ideas, events, and interests with others, even with influential people or organizations.[5] By allowing the free flow of communications in all directions, social network sites break down traditional social boundaries.

SOCIAL NETWORK SITES (SNS) AND A BRIEF HISTORY OF SOCIAL MEDIA

Some examples of social network sites include Facebook, MySpace, LinkedIn, Tumblr, Twitter, YouTube, and Pinterest. Although some SNS appear to be new or revolutionary, earlier predecessors have heavily influenced each site. Understanding the roots and history of online social networks also assists in the understanding of their significance in our discussion.

The earliest SNS cropped up in the late 1990s. SixDegrees.com and Classmates.com were some of the earliest social networking sites. While each site had its own focus, both allowed its users to connect to others online, utilizing varying forms of profiles and lists of friends or old classmates. Despite innovations, most people at the time did not have large networks of friends who used the Internet frequently. The founder of SixDegrees argued that the site was "ahead of its time."[6]

During the early 2000s, social network sites like Ryze.com, Tribet.net, LinkedIn, and Friendster appeared. All four were created among developers who knew each other personally and professionally. They believed they could all co-exist and support each other rather than directly compete with one another. Out of the four sites, LinkedIn became one of the most successful; it grew into a powerful business-networking site. Friendster grew quickly, but failed to keep its popularity; however, its model heavily influenced subsequent social network sites.[7]

Soon after this period, Pyra labs sold Blogger to Google, which was initially only an online search engine company. Blogger was one of the early web applications for creating

[5] "Social Media for Intelligence…"

[6] Boyd and Ellison, "Social Network Sites…"

[7] Ibid.

and maintaining weblogs or “blogs.” This allowed almost anyone with a computer and Internet access to post their own thoughts, stories, pictures, and ideas to whomever online.

By the mid-2000s, more Internet users facilitated the growth of SNS. In 2003, MySpace launched and was intended to compete with Friendster. It too utilized the format of profiles, lists of friends, and allowed users to upload picture and to edit their own profiles using html. The site gained popularity at first with “Indie” (independent) music groups and their fan bases. As a result, it then extended to teenagers and young adults.

Soon after, in early 2004, Facebook launched as an exclusive Harvard-only site. It too employed the use of profiles, lists of friends, but focused on the academic spheres of its users lives: lists of courses, clubs, and organizations. It soon expanded to other university students; only those with .edu email accounts were able to sign up for the service. It then opened up to high school students and professional organizations. Eventually, it opened up to everybody and its popularity skyrocketed as one of the most popular and valuable SNS to date.

In 2005, three former PayPal employees launched a video-sharing site and named it “YouTube.” YouTube allowed users with profiles to upload their own videos and view other publicly posted videos. This led to a democratization of reportage and video documenting in extraordinary ways. Google purchased YouTube in 2006 for $1.65 billion in stock and have made it into one of the most popular sites in the world. This will be further discussed in the file sharing section below.

The mid to late 2000s in addition to the early 2010s saw the rise of other social media platforms: Twitter, Tumblr, Flickr, Google+, Foursquare, Reddit, Pinterest, Spotify, Instagram, FeedBurner, Optify, WordPress, and Pinterest. Although these platforms have varying purposes, they all bring people into a network online through the use of profiles, lists of friends, or interests. By examining the different platforms of social media, many of their intended uses will become apparent.

It is also crucial to note that during the creation of these U.S.-based social network sites, that there were also sites that were created to cater to foreign users (whether intentionally or unintentionally), especially in countries such as China. Sites such as

Cyworld, Badoo, Haboo, Orkut, and QQ have individually attracted many hundreds of millions to likely over a billion collective users from around the globe since their creation.[8] To only focus on the social networking sites popular in the U.S. would create a narrow and incomplete picture of the online social networking landscape. Especially in our context of typically foreign enemies, Islamic terrorists, and Mexican drug cartels, the inclusion of these other SNS are necessary. If US law enforcement and intelligence community people are not familiar with US social media like Twitter and Facebook, the chances that they are deeply familiar with sites such as QQ is probably fairly predictable.

BLOGS AND MICROBLOGS

Under the umbrella of social media, are also "blogs," originally known as web logs, but with the words combined into the current word. The prevalence of weblogs or blogs appeared in the late 1990s. Computer-savvy individuals, who had to code their own pages using HTML, authored most of the early blogs. Nevertheless, soon, free online blog platforms became available to everyone, even if the individual was not proficient in coding language.[9] As mentioned, Blogger was one of the first online blog publishing platforms. There are also other popular blog platforms such as WordPress, and Xanga.

To better explain, a blog is a website maintained by an individual or small group, who regularly post "commentary, descriptions of events, or other material including graphics or video."[10] Blogs are typically disseminated using RSS services to frequently publish the bloggers' updated works. Blogs have also extended beyond written entries to photo, audio, or video formats and are both open and closed---closed sites are only open to certain people and represent one of the simplest ways of sharing data outside the view of most law enforcement and intelligence community discovery or monitoring.

Bloggers, the authors of blogs, have changed the world of traditional media outlets, namely newspapers, magazines, and television by allowing people to bypass these traditional

[8] "Alexa Top 500 Global Sites," *Alexa*, accessed February 2, 2012, http://www.alexa.com/topsites.

[9] Carolyn Miller and Dawn Shepherd, "Blogging as a Social Action: A Genre Analysis of the Weblog," *Into the Blogosphere: Rhetoric, Community, and Culture of Weblogs*, last modified November 30, 2004, http://blog.lib.umn.edu/blogosphere/blogging_as_social_action_a_genre_analysis_of_the_weblog.html.

[10] "Social Media for Intelligence…"

forms. "Self-expression is a salient theme among some bloggers, who find the same opportunity that television talk shows afford their participants: the opportunity to tell their stories in a mediated forum to a potentially large, though distant and invisible, audience."[11] As bloggers are given a platform from which to voice their opinions, research and "report," people find more sources of news and information online. This has also made it possible for niche communities of followers to form around not-so-mainstream ideas or interests, whether it is gothic fashion or Islamic extremism.

Closely linked to blogs are microblogs. These include Twitter and Facebook status updates. Microblogs are typically 140 characters or less; this was inspired by the limit imposed on SMS text messages sent on cellular phones. Status updates or tweets are different from traditional blogging with not only their length, but also their frequency. Similar to blogging, microblogging typically provides means for readers to subscribe to a user's updates. The world of Twitter and microblogging has extended to prominent individuals in society, businesses, and the average person wanting to express their day-to-day, hour-to-hour thoughts.[12]

Although the idea of microblogging may often come across as narcissistic, (celebrities such as Lady Gaga announced to her over 21 million followers that she was taking a vow of silence) it can provide real-time information and general attitudes of different peoples and populations. Sites such as Twitter and Facebook were closely monitored during recent crises such as the Mumbai attacks, the Arab Spring, and the Japanese earthquakes and tsunamis. Media outlets and governments used these sites to gain insight into the actions and attitudes of average citizens, especially those in the specific areas of interest for the event such as Mumbai or near the home of Osama bin Laden. To understand the impact of microblogging sites such as Twitter, there are well over 200 million tweets a day. This number continues to escalate.[13]

[11] Miller and Shepherd, "Blogging as a Social Action…"

[12] Scott Nesbitt, "What is Microblogging?" Tech Tips, *Geeks.com*, last modified April 26, 2009, http://www.geeks.com/techtips/2009/what-is-microblogging.htm.

[13] "Social Media for Intelligence…"

FILE SHARING

File sharing is the “public or private sharing or providing access to digitally stored information.”[14] The types of files include data files such as documents, spreadsheets, and presentations. File sharing services can also include audio in MP3 file formats, video, images, and links to other online content. Some of the more popular file sharing social media platforms include: YouTube (video sharing), Google Doc (interactive document and spreadsheet sharing), Flickr (image sharing), SlideShare (presentation slide sharing), Spotify and Playlist (music sharing), Pinterest (link and image sharing), and Dropbox (large file sharing).

Some of these file-sharing platforms also cross over into social network territory such as YouTube, Flickr, Pinterest, Spotify, and Playlist because they utilize profiles and create networks of “friends” or subscribers, who have similar interests. Burgess and Green called YouTube “a high-volume website, a broadcast forum, a media archive, and a social network.” These sites are more than simple file sharing platforms, but are connecting its users and forming communities online. Moreover, these sites are changing the way society saves and shares information.

Since YouTube’s founding in 2005, it has changed who plays the ‘gatekeeper’ to video media. Prior to YouTube, network broadcasting, Hollywood, and cable networks controlled most video media and determined what people viewed. Now, YouTube allows any individual (or company) to share whatever content, as long as it does not infringe upon copyrights or goes against its Users’ Terms of Agreement. The site has made obscure people into overnight celebrities, like recording artist Justin Bieber, whose career was generated after his mother posted videos of Justin singing and performing. He is now a worldwide sensation thanks to YouTube’s platform.

Not only does the site create celebrities, but it also brings awareness to issues. Videos show everything from police misconduct to riots in the Middle East to underage drug usage to gang violence. The effect of YouTube is incalculable; however, we can observe the magnitude of its influence in several cases. For example, in January of 2012, a video was leaked onto YouTube showing four U.S. Marines urinating on Taliban corpses in

[14] “Social Media for Intelligence…”

Afghanistan. The video enraged not only Afghanistan's population, but the international community condemned it. This severely hurt America's relations with Afghanistan's leadership.[15] More examples of YouTube's influence will be discussed in Chapter 2.

GEO-LOCATIVE SOCIAL MEDIA / LOCATION-BASED SITES

Locative social media or location-based sites "provide status updates linking content with the [data] of a user's geographic location."[16] Some examples include Foursquare, Facebook Places, Scvngr, and even Google Earth that provide both location and social features to share through forums, blogs, or maps. Locative media often uses the GPS features of a mobile device, such as a smartphone with software linked back to infrastructure and servers such as Google Latitude which uses the location information to share with specific people or services opted-in by the originator. These platforms allow users to share with their friends where they are, when they go there, and how often they frequent these locations. Applications, such as Foursquare, award its users for "checking in" into locations with badges and reward points. Facebook Places provides a map of the location, a list of friends who are also checked in at the location, and past friend visit activity. These services "can provide a pattern of behavior linked to the quantity and location of content updated from mobile devices."[17]

Many services such as Twitter enable location, making the service into GeoTwitter and enabling many aspects of crowdsourcing and data analytics that can be of immense importance to both law enforcement and the intelligence community. Unintentional location information such as the meta-data in many pictures posted on the Internet have given criminal groups such as sexual predators an enormous amount of information about where children are, where women are, and a host of other unintended results of sharing the location of information. The FBI issued an alert on this location meta-data from phones, but few

[15] Graham Bowley and Matthew Rosenberg, "U.S. Deplores Video of Marines Urinating on Taliban," *The New York Times*, January 12, 2012, http://www.nytimes.com/2012/01/13/world/asia/video-said-to-show-marines-urinating-on-taliban-corpses.html?pagewanted=all.

[16] "Social Media for Intelligence…"

[17] Ibid.

people are aware of the enormous risk involved in photo sharing from GPS-equipped smartphones.[18]

The personal nature of this information has raised privacy concerns. Incidents of crime have occurred due to the voluntarily provided information. A report from Credit Sesame, which interviewed 50 ex-burglars in England, found that 78% of the robbers used Facebook, Twitter, Google-Street View, and Foursquare to check for potential targets. In fact, three robbers in New Hampshire utilized Facebook status updates and were able to steal items valuing over $200,000.[19] Further implications of locative social media will be expounded upon in Chapter 2.

VIRTUAL WORLDS, ONLINE GAMING, AND SOCIAL GAMING

Virtual world or online gaming is another social media platform is worth discussing when examining social media and nefarious groups. These include games such World of Warcraft, Second Life, and Call of Duty, where players can connect to other players around the world with the aide of the Internet. The players typically utilize pseudonyms and not only play the games, but interact socially with others around the world, which are also playing. The activity is very much a social activity, which these games are included as types of social media platforms.

In 2010, online gaming became the number two online activity for Internet users, which surpassed even email usage. Online gaming came in second to social network sites. Though online gaming and has been considered disparate, they are increasingly merging into an enormously profitable market. Some of the online gaming has converged into what is coined as "social gaming," where users play games through applications on social network sites such as Facebook. Facebook games, Farmville and Mafia Wars amassed revenues in excess of $500 million in 2010. The Internet and now social network sites have taken the

[18] "FBI Friday: Be Prudent When Posting Images Online," *ProtectMyID* (blog), April 13, 2012, http://blog.protectmyid.com/2012/04/13/fbi-friday-be-prudent-when-posting-images-online/.

[19] Boonsri Dickinson, "Infographic: 80% of Robbers Check Twitter, Facebook, Google Street View," *Smart Planet*, last modified November 1, 2011, http://www.smartplanet.com/blog/science-scope/infographic-80-of-robbers-check-twitter-facebook-google-street-view/11082.

once solitary or isolated activity of computer gaming and has morphed it into an online community, where gamers connect, make friends, and essentially socially interact.[20]

DEMOGRAPHICS OF SOCIAL MEDIA USERS, FREQUENCY OF USAGE, AND FEATURES UTILIZED

After covering the history and uses of social media, it is noteworthy to examine who actually uses these services and how they are used. In June 2011, the Pew Research Foundation conducted a comprehensive survey of Americans and their usage of SNS. Information that is relevant in the examination of SNS, clandestine groups, intelligence gathering, and law enforcement will be summarized below---but the growth of SNS is very rapid that these statistics are out-of-date almost before they are published.

In examining the demographics, the survey reveals that 79% of U.S. adults use the Internet and nearly half of those users (47%), or 59% of actual Internet users, say they use at least one SNS. This number doubled from 2008, when it was at 35%. This demonstrates the rapid growth and wide usage of the Internet and SNS.[21]

The survey also researched the average age and sex of SNS users. The survey demonstrated that the average age of SNS is actually increasing: over half of SNS users today are over the age of 35. The survey also showed the average age of varying SNS platforms. For example, the average MySpace user is younger (32), the average LinkedIn is older (40), the average Facebook user (38), Twitter (33), and all other SNS (35). Except for LinkedIn, almost all the popular social media platforms have more female users than male users. For example, females are disproportionately (56%) more likely to instant message, blog, and photo share.[22] These statistics continue to change and demonstrate the irreversible importance of social media in the lives of people globally---though few global statistical surveys are available, as services such as QQ in China are enormous, but much more closed

[20] Ethan Lyon, “Emergence of Online Social Gaming,” *Sparxoo*, last modified August 2, 2010, http://sparxoo.com/2010/08/02/nielsen-study-social-gaming/.

[21] “Who uses what social networking site platform,” Pew Internet & American Life Project, *Pew Internet*, accessed February 2, 2012, http://www.pewinternet.org/Reports/2011/Technology-and-social-networks/Part-2/Platform.aspx.

[22] Ibid.

with their usage statistics (though in 2011 more than 700 million people used this instant messaging service in China).[23]

Pew Research also looked into how frequently Americans are using social media and what features they typically use of these platforms. It found that Facebook is, by far, the most popular SNS. Of those who use SNS, almost all (92%) use Facebook. After that, MySpace (29%), LinkedIn (18%), Twitter (13%), and all other (10%). The survey also found that Facebook and Twitter are used more frequently than MySpace and LinkedIn. It showed that 52% of its users access Facebook daily and 33% access Twitter daily.[24] These statistics continue to change markedly each year as services like Facebook and Twitter and Google+ become dramatically more capable and indispensible in most people's lives. Figure 1 is an example of the speed of growth of these services is the relative time it took for Facebook (852 days), Twitter (780 days), and Google+ (16 days) to reach 10 million users.[25]

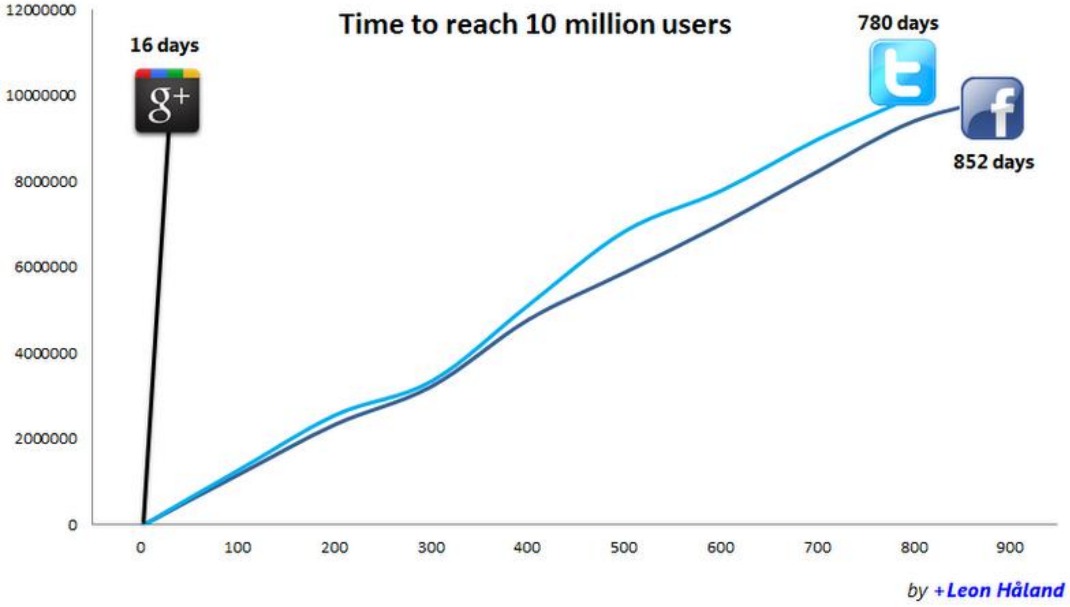


Figure 1. Time to reach 10 million users. Source: Håland, Leon. "Time to Reach 10 Million Users." *Google+*. Last modified September 30, 2011. https://plus.google.com/112418301618963883780/posts/D2Rz5rdciWE.

[23] "Tencent QQ," *Wikipedia*, last modified March 30, 2012, http://en.wikipedia.org/wiki/Tencent_QQ.

[24] Ibid.

[25] Paul Sawers, "Google+ Reached 10m Users in 16 Days. Want to Know How Long it Took Facebook and Twitter?" *The Next Web*, last modified July 22, 2011, http://thenextweb.com/google/2011/07/22/google-reached-10m-users-in-16-days-want-to-know-how-long-it-took-facebook-and-twitter/.

In regards to the types of usage on these platforms, the survey demonstrated that on Facebook, 15% of users update one's own status, 22% comment on others' posts or status, 20% comment on another user's photo, 26% "like" anther user's content, and 10% send other users a private message. As far as the age and sex demographics of private messaging, there is no real difference in usage between male and females; however, younger users are more likely to send private messaging.[26]

What does this data suggest? First, it suggests that not all platforms are created equally. All SNS should not be treated similarly. This information could aid law enforcement and intelligence officials when dealing in intelligence gathering and investigations. Instead of subpoenaing LinkedIn for information on a 20 year-old, non-college graduate suspect, energy can be better spent on MySpace or Facebook according to this type of data. More information could be gathered such as SNS used abroad, which would be useful in intelligence gathering and even law enforcement involving smuggling or trade. Consistent updates of these types of numbers will also clue government officials as to the trends of which social media platforms Internet users are using.

To gain an up-to-date snapshot of what is currently popular and avoid the costs of surveys, sites such as Alexa, a web-information company, provides the rankings of the most popular websites. It provides each sites' traffic stats, demographics of its audiences (users' age, gender, education, and browsing location), reviews, and reputation. For an additional cost, a user can have access to more extensive demographic information: such as income or ethnicity of the audiences. An example of the type of data Alexa provides, as of early 2012, Google.com was ranked as the number one accessed nationally and globally. It ranked Facebook number two in both areas also. It shows that the browsing location of Google and Facebook users relative to general Internet population, are browsing from school more than other locations.[27] This data is crucial to capturing a snapshot of current trends online and to better understanding social media. Moreover, this current data could also act as variables in social media monitoring systems, a topic, which will be expounded upon in following sections.

[26] Sawers, "Google+ Reached 10m Users…"

[27] "Alexa Top 500 Global Sites."

SOCIAL MEDIA'S SOCIAL IMPACT

It is undeniable that social media has had a social impact. It has changed the way in which we communicate with one another. Its free and convenient usage has shifted away from the usage of traditional forms of communications and media like telephones (even cellular phones), emailing, newspapers, and television.

The emergence of online social media has also transformed the manner in which we share personal information. Albrechtslund argued that social networking online "seems to introduce a participatory approach to surveillance." In his article, he cited Gross and Acquisiti, "While privacy may be at risk in social networking sites, information is willingly provided." The motivation behind this "information revelation" is typically caused because the user considers the "perceived benefit of selectively revealing data to strangers may appear larger than the perceived cost of possible privacy invasions." These include peer pressure or "herding behavior, relaxed attitudes or apathy towards personal privacy, and/or faith in the networking service or trust in the users.[28] Regardless of users' willingness to share personal information online, they are doing so and this vast trove of information is powerful if properly utilized.

SNS have also altered our own social networks and how we associate and communicate with others. SNS communities often reflect communities and relationships in real life; however, these sites can also foster communities online that would not have existed because of the location or members or the illegal nature of these acquaintances. SNS's global presence indeed allows us to stay in touch with people more easily regardless of their location. Social media links people around the globe with common experiences, interests, and ideologies. In Chapter 2, how social media is used to mobilize people around the world is discussed, as is how social media facilitates the associations of members in clandestine groups.

The answer to why we should concern ourselves with social media when discussing law enforcement and intelligence gathering is simple: the threats and enemies of the nation are using SNS. This study focuses on two types of clandestine groups, terrorist groups

[28] Anders Albrechtslund, "Online Social Networking as Participatory Surveillance," *First Monday*, last modified March 3, 2008, http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2142/1949.

(namely Islamic terrorist groups, such as al-Qaida) and Mexican drug cartels. These groups represent the subjects of both investigations and of intelligence gathering. Both these types of groups are of great interest to U.S. law enforcement and intelligence bodies and as such, are a focal point of this paper. Many other groups such as white supremacy organizations, Internet groups such as Anonymous, and sexual trafficking and exploitation groups could easily be added to the discussion and clearly to the concerns of law enforcement and the intelligence community.

Social media monitoring is becoming crucial to today's efforts to protect the U.S. It is extraordinarily unwise and actually naive to believe it can be ignored or neglected or that it will somehow pass as a fad. With online social media playing a larger role in people's lives, a large piece of the puzzle will be missing if it is dismissed in investigations or intelligence gathering. This author has witnessed firsthand how the application of social media surveillance can bring greater understanding in an investigation and also how often it is overlooked. Both the law enforcement and IC must continually keep themselves current on social media in order to be most effective. Nevertheless, we have seen how SNS have changed the approaches of intelligence gathering and law enforcement. Governments have already taken interest and it is obvious why. Albrechtslund stated:

> To profile potential criminals and terrorists, it is necessary to combine a wide range of information about people. This information includes social relations, such as shared activities and circles of friends as well as personal data about political views, religious beliefs, sexual orientation, and preferences regarding everyday life activities.[29]

In most cases, the users have openly and freely provided this information. SNS users have done the work for government officials and any interested individual. The information is easily available and searchable, which will be demonstrated in Section 3. Developing ethical social media monitoring facilitates the concept of "connecting the dots" since the personal data is already available, whether from one or a combination of multiple sources.[30] This

[29] Albrechtslund, "Online Social Networking…"

[30] Ibid.

information is essentially available to everyone, but whoever "is the best at deriving insight from that information has the intelligence advantage."[31]

Not only are SNS providing "raw data" about individuals' lives, but they also provide better understanding. The open-source social media information "complements and provides context to traditional media sources" and traditional forms of communications."[32]

[31] "Social Media for Intelligence…"

[32] Ibid.

CHAPTER 2

THE EXPLOITATION OF SOCIAL MEDIA BY TERRORIST GROUPS AND DRUG CARTELS

After the September 11th attacks, Osama bin Laden boasted that he had hundreds of men willing to die and also hundreds of Muslim scientists who would use their "knowledge in [. .] computers [and] electronics against the infidels."[33] His threat was realized through the utilization of social media. Federal law enforcement and intelligence agencies have publicly recognized the exploitation of social media by terrorists and criminal groups such as drug cartels. The Federal Bureau of Investigation's (FBI) executive Assistant Director for the Science and Technology Branch stated:

> We have detected the use of social networking and multimedia websites by terrorists and have confirmed that they are using those forums for recruiting, communications, and the distribution of propaganda."[34]

In addition to communication and recruitment, these websites are used for cybercrime, fundraising, money laundering, and counterintelligence gathering. Although criminal groups typically have financial motives rather than the political motives of terrorists, they utilize these sites for similar purposes.

COMMUNICATION

Social media and online social network sites have altered how the world communicates. As such, clandestine groups have also adapted to the new technologies; this has altered their forms of communications. The accessibly of social media sites allows gangs

[33] Dan Verton, "Virtual Threat, Real Terror: Cyberterrorism in the 21st Century," Errata: Dan Verton, accessed March 4, 2012, http://attrition.org/errata/sec-co/danverton-02-testimony.html.

[34] Ronald Kessler, "Facebook, YouTube, and Terrorists—A Deadly Mix," *Newsmax*, last modified February 18, 2011, http://www.newsmax.com/RonaldKessler/Facebook-YouTube-FBI-Terrorists/2011/02/18/id/386589.

and other criminal groups to easily communicate and even form alliances nationwide and worldwide.[35]

The decentralized nature of the Internet mirrors the decentralized and franchised nature of terrorist organizations like al-Qaida and its operations.[36] As a result, the user-generated and updated social media platforms bode well with the globally dispersed group. Thirteen years ago, Professor Gabriel Weimann from the Haifa University in Israel, began monitoring Internet sites utilized by Islamic terrorist groups. He observed that groups like al-Qaida are increasingly becoming sophisticated in their use of social media platforms like YouTube, Twitter, MySpace, Facebook, and other sites.[37] Social network sites also work well with criminal groups such as drug cartels, which have a scattered network of suppliers and distributors across the globe.

Facebook and regional equivalents offer free, accessible, and convenient means of staying connected with a network of friends. Members of clandestine groups use SNS for personal and "business" purposes. The free services provide another means of communication within a group or network of conspiring individuals. The ability to adapt a new persona or attain anonymity offers a certain level of protection from law enforcement and intelligence agencies. Clandestine groups benefit from the relative anarchy in cyberspace. Evan Kohlmann, who has spent over a decade tracking terrorist groups online, stated the "most important social networks are being formed entirely online" considering the Internet provides anonymity, interactivity, and a "resilient infrastructure." Regardless of where the individuals are in the world, they can be instantly connected, who sympathize with the same cause.[38]

[35] "2011 National Gang Threat Assessment," *National Gang Intelligence Center*, accessed February 2, 2012, http://www.fbi.gov/stats-services/publications/2011-national-gang-threat-assessment/2011-national-gang-threat-assessment-emerging-trends.

[36] John Rollins, "Terrorist Use of the Internet: Information Operation in Cyberspace," CRS Report, accessed October 2, 2011, http://www.fas.org/sgp/crs/terror/R41674.pdf.

[37] "Terrorism at Work in Social Networks," *NTD Television*, accessed February 13, 2012, http://english.ntdtv.com/ntdtv_en/news_middleeast_africa/2012-01-24/terrorism-at-work-in-social-networks.html.

[38] Gina Vergel, "Security Expert: Social Networking Sites are Hotbeds of Terrorism," *Fordham University*, accessed February 13, 2012, http://www.fordham.edu/Campus_Resources/eNewsroom/topstories_1916.asp.

For example, when signing up for a service like Facebook, the individual has relative freedom of providing a false or incomplete name to the company. Although false names are against the user's Terms of Agreement, it is easily accomplished. In more traditional law enforcement, the discovery or seizures of telephone numbers enables agents and analysts to subpoena or court order a phone provider and request subscriber information for a specific phone number. Unless the user is using a prepaid cellular phone, the subscriber information typically contains the user's name, address, billing address, cell phone serial number, email addresses, and alternate phone numbers. Nevertheless, when subpoenaing or court ordering a social network company, the information is incomplete considering users are not required to offer any in depth information. Although companies may provide law enforcement with IP addresses from which the users are accessing their accounts, the existence of cyber-café's and the ability to manipulate the actual IP address, law enforcement is left with little information on the user's actual identity.

Cyber space has simplified and eased the ability of terrorist groups and drug cartels to communicate within their respective groups. A shift away from traditional landlines and even cell phones has made the work of law enforcement more difficult. Moreover, the plethora of SNS options for these groups leaves law enforcement scrambling as it struggles to adapt and keep up with the ever-changing landscape of cyber communication.

YouTube channels and Facebook pages also create a line of communication between networks of terrorist organization and possible Western-based sympathizers and "lone wolf" actors. The ability to connect with those across the globe provides "moral" support for "lone wolf" terrorists in the West.[39] These sites facilitate information transmission and material support for acts of terrorism. In a case involving a U.S. citizen, who lived in Pennsylvania, the woman allegedly used the nickname "JihadJane" to post jihadist messages on YouTube, in jihadist chat rooms, and websites in order to "plan and facilitate an overseas attack."[40] [41]

[39] Rollins, "Terrorist Use of the Internet…"

[40] Ibid.

[41] Carrie Johnson, "JihadJane, an American Woman, Faces Terrorism Charges," *The Washington Post*, March 10, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/03/09/AR2010030902670.html.

In addition to the more popular sites like YouTube and Facebook, Congressional members have been concerned about other social network sites becoming cyber grounds for terrorist communication and operation planning. In order to address the issue, in 2008, Congress held a hearing on the potential dangers of virtual communities like Second Life. Second Life, is a virtual world, where users' avatars (graphical representations) interact with other users. Users are anonymous and can communicate with one another using text and voice chat.

Members of Congress were not alone in their concerns. The National Gang Intelligence Center also believed in the virtual world's potential danger and stated that Second Life "provides versatility and anonymity and allows for covert communications." The Center added that with the anonymity and versatility, gang members could recruit, spread propaganda, commit crimes like drug trafficking, and receive training for real-life criminal operations.[42]

Regardless of the reports and testimonies at the Hearings concerning Second Life's vulnerability to terrorism, the founder of Second Life believed Congress overreacted. Philip Rosedale, the founder, testified, "Though there has certainly been discussion [about terrorism in virtual worlds], we have never seen any evidence that there is any such activity going on in Second Life." Moreover, he added that Second Life would actually not be attractive to terrorists considering how closely members' activities are monitored. He argued that the virtual world is "somewhat more police-able" than covert activities in the real world.[43] Critics from computer and technology circles also agreed that the likelihood of terrorists taking advantage of Second Life was unfounded especially taking into account the virtual world's decline in popularity.[44, 45]

Although Second Life has fallen out of the limelight in recent years, it continues to have an estimated one million users who log in every month. Despite criticism of Congress's

[42] "2011 National Gang Threat Assessment"

[43] Chloe Albanesius, "Terrorists in Second Life? Hogwash says CEO," *PC Magazine*, April 1, 2008, http://www.pcmag.com/article2/0,2817,2280660,00.asp.

[44] Sharon Weinberger, "Congress freaks out over Second Life," Danger Room, *Wired*, last modified April 4, 2008, http://www.wired.com/dangerroom/2008/04/second-life/.

[45] Albanesius, "Terrorists in Second Life?…"

overreaction, if users are still utilizing the virtual world, perhaps it should not be entirely ignored or overlooked.

It is not only Second Life that has caused concern. Congress, the U.S. military, and intelligence community have also grown concerned about the World of Warcraft multiplayer online game. They have grown concerned that the game makes "it incredibly easy to gather plotters from around the world. But mostly, virtual worlds are nerve-wracking to spies because they're so hard to monitor." Users of games, such as World of Warcraft, use pseudonyms, use heavy jargon, and access the game from around the world.[46]

At the 2008 Director of National Intelligence Open Source Conference, Dr. Dwight Toavas, a professor from the National Defense Academy, presented a fictional scenario in which gamers (users) utilize World of Warcraft as a planning tool to attack the White House. The demonstration was filled with jargon to somewhat mirror an actual gaming scenario. The plotting gamers used maps inside the game as substitutes for their target maps. The scenario was meant to demonstrate how the World of Warcraft could be used as n effective communication, planning, and coordination tool for terrorist attacks.[47]

Although critics have argued that the intelligence and military community have overreacted to this threat, it became evident in 2011 that their predictions were not unfounded. In 2011, Norwegian Anders Behring Brejvik killed seven people in a bomb attack and shot 86 people in a Norwegian youth camp. He claimed in a 1,500-page manifesto that he used the game World of Warcraft and Modern Warfare 2 to stage and practice before his attack.[48] Brejvik's plot, which used online gaming during the preparations, is a realization that these online gaming platforms can indeed be used for malicious intents.

Drug cartels have proven a high level of sophistication in their communication systems. Some drug cartels have even taken on state-like sophistication. An anonymous journalist from Nuevo Laredo commented, "The narcos have people who are experts in

[46] Noah Schachtman, "Pentagon Research Conjures Warcraft Terror Plot," Danger Room, *Wired*, last modified September 15, 2008, http://www.wired.com/dangerroom/2008/09/world-of-warcra/.

[47] Ibid.

[48] "Norway Killings: Shooter Used Video Games as Training Methods," *International Business Times*, last modified July 27, 2011, http://au.ibtimes.com/articles/187509/20110727/anders-behring-brejvik-activision-modern-warfare-world-of-warcraft-norway-killings.htm.

communications."[49] For example, the drug cartel, which is made up of former members of the Mexican military Special Forces, the Zetas, has highly sophisticated communication. Instead of relying on vulnerable communication infrastructure on which to communicate, the cartel has built their own sophisticated infrastructure "to aid with both command-and-control operations and [receive] early warnings about police or military interventions."[50] The ability to send encrypted messages over a controlled cellular phone network prevents police and military officials from cracking into the group. The cellular network could most likely have social network site access. The private communication network effectively prevented government officials from obtaining any cellular information until the Mexican government eventually destroyed the communication systems.

Although the Zeta cellular communication is an extreme in drug cartel sophistication, many cartel members use social network sites for both personal and business purposes. In 2010, *Time* magazine reported on the use of both Facebook and Twitter by drug cartels. Mexican officials believed that the groups had been using sites like Facebook to facilitate in the kidnappings of powerful politicians and businessmen's relatives. By simply viewing the profiles of the prominent people, cartel members discovered the identities of the relatives' names along with their pictures.[51]

Moreover, Twitter has been used to disseminate information in the cartel communities. Ghaleb Krame, a security expert at Mexico's Alliant International University, stated that these criminal groups communicate among themselves through the use of code words on social media sites. For example, on YouTube, cartels post videos of *corridos* or ballads, with lyrics that "contain subtle clues as to the current hierarchies of gangs—as well as threats."[52]

[49] "Mexican Social media boom draws drug cartel attacks," *Reuters*, last modified September 27, 2011, http://www.reuters.com/article/2011/09/27/us-mexico-drugs-idUSTRE78Q6H220110927.

[50] Mark R. Yzaguirre, "Drug Cartels get more sophisticated," *FrumForum*, last modified January 3, 2012, http://www.frumforum.com/drug-cartels-get-more-sophisticated.

[51] Alexis Okeowo, "To Battle Cartels, Mexico weighs Twitter Crackdown," *Time*, April 14, 2010, http://www.time.com/time/world/article/0,8599,1981607,00.html.

[52] Ibid.

In addition to the known uses of social media by terrorist and criminal groups, there are endless possibilities of how they could covertly communicate. Because file-sharing platforms are discreet in nature, they present a potential problem for law enforcement and intelligence officials. For instance, Google Docs, which allows users to publicly share documents, also permits users to share their documents with only an invited set of users. The author of the document can designate authority to other users in the group to edit and as such, multiple users are able to edit a document in real-time. File sharing poses two problems: suspicious documents can be easily shared without detection of government officials and real-time conversations can occur far from any scrutiny. Unlike emails, online social network interactions, and even instant messaging online, government entities such as the NSA are less likely to intercept such conversations and interactions on file sharing sites.

Another file sharing platform, which also has potential to become a tool in terrorist or criminal groups' hands is a site called Thingiverse. Thingiverse is an online community that allows users to upload and share "potentially useful 3D models for others to print out at home" using 3D printers. These 3D printers have become increasingly more affordable in recent years. A user on the website "posted the plans for printing a magazine for an AR-15 rifle." Although the plans he printed were not for an illegal weapon, his plans were easily modified for a magazine that would hold fifteen instead of five rounds of ammunition, which would render it illegal. In response to the post, another user on Thingiverse "posted a model for printing a part called the lower receiver for the AR-15."[53] The lower receiver is the only part on the AR-15 that cannot be purchased from "gun shows or mail-order catalogs," which do not always keep record of purchases. As such, "By printing out the lower receiver of an AR-15 on a 3D printer, it's possible to complete construction [of] a fully functional, unregistered AR-15."[54] The 3D-printing technology coupled with file-sharing sites like Thingiverse could become extremely valuable to criminals and terrorists who want to fly under the radar in their arms purchases.

[53] David Daw, "Criminals find new uses for 3D printing," *PC World*, Last modified October 10, 2011, http://www.pcworld.com/article/241605/criminals_find_new_uses_for_3d_printing.html.

[54] Ibid.

3D printers have also been used to print copies of police handcuff keys (with the model available online) and ATM skimmers, which steal debit or credit card information at ATM machines. As technologies continue to advance and evolve, there is no limit as to how nefarious groups can exploit every new turn of advancement.[55]

PROPAGANDA AND RECRUITMENT

SNS are not only used for only communicating among existing members, but are also used to recruit and propagandize. SNS is a simple and free medium for propaganda. Sites such as Twitter enable terrorists to anonymously communicate with a larger audience in real-time. Tom Osborne, unit chief of the FBI's Counterterrorism Internet Targeting Unit (CITU) stated, "Social networking sites certainly can and do provide a means to bring like-minded individuals together whether it is for radicalization, recruitment, or other terrorism objectives."[56]

Before the rise of social media sites, terrorist groups put up radical websites waiting for curious and sympathetic "customers." Weimann noted, "instead of waiting [for] the customer to come to the propaganda shop on-line, they [terrorists] are pushing the product into the social network."[57]

In 2010, the Simon Wiesenthal Center for Tolerance released the 2010 Digital Hate Report. The report found a 20% increase in hate-filled social networks, websites, blogs, Twitter feeds, Facebook posts, etc. The report noted the trend of terrorists at targeting younger people through the use of SNS and online violent video games. One example, was a video game which invited users to bomb Haitian earthquake victims. Others examples included how-to videos for aspiring terrorists. Some of the videos demonstrated how to build bombs and some even included information on binary and laser technology. The report also found the increasing promotion of the role of "lone wolf terrorists" by terrorist groups.

Radical jihadist groups in the U.K. have also been using Facebook and other social network platforms to recruit and disseminate extremist literature. In 2008, it was reported

[55] Daw, "Criminals find new uses…"

[56] Hoda Osman, "Alleged Terrorists Used Social Network Sites," *CBS News*, May 19, 2010, http://www.cbsnews.com/8301-31727_162-20005405-10391695.html.

[57] "Terrorism at Work in…"

that a private Facebook group called Ahlus Sunnah wal Jama'ah, had been operating for over a year. The group had posted web links to extremist literature by jailed radical leaders Abu Hamza al-Misri and Abu Qutada calling for armed jihad against both American and British governments. The group also demanded the expulsion of any Muslim who voted in elections or "provided assistance" to "non-believers."[58] The leader of Ahlus Sunnah wal Jama'ah, Anjem Choudray, did not claim any link or responsibility for the Facebook group, but admitted that his organizations "widely" used social network sites to recruit support.

In 2008, detailed plans on how al-Qaida is seeking to use social networks, such as Facebook, for propaganda purposes were leaked onto a public message board and translated. The plans called for "brigades," which would spread videos of suicide bombers and written accounts of martyrs. Military training manuals and step-by-step videos would also be planned by using special Facebook "applications," which can convert them into English from Arabic. Last of all, one of the users of the message board, al-Faloja, remarked, "Facebook is perfect for reaching young people and fight the media." Also that they have "already had great success in raiding YouTube, and the next target is to invade Facebook."[59]

Al-Qaida's exploitation of YouTube has been evident. The group's uploaded videos of tortured captives and executions are a part of its propaganda plan. YouTube has been exploited as a tool for "'soft' psychological warfare" where they post "militants boasting accomplishments and [create] an aura of a successful group that others may want to join."[60] Kohlmann noted that it is easy to forget that YouTube is more than just a website on which to upload and watch videos, but is a vibrant online community and forum of participating users. The website is interactive. Users can "subscribe each other's feeds based on mutual interests," like al-Qaida or radical Islam.[61]

[58] "Terrorists recruiting on net via Facebook," *Scotsman*, last modified February 16, 2008, http://www.scotsman.com/news/terrorists_recruiting_on_net_via_facebook_1_1429940.

[59] "Al-Qaeda Plans to Wage Holy War on Facebook," *The Telegraph*, December 21, 2008, http://www.telegraph.co.uk/news/worldnews/3885367/Al-Qaeda-plans-to-wage-holy-war-on-Facebook.html.

[60] Doug Bernard, "Does Social Media Help or Hurt Terrorism?" *Voice of America*, last modified January 21, 2012, http://blogs.voanews.com/digital-frontiers/2012/01/21/does-social-media-help-or-hurt-terrorism/.

[61] Evan F. Kohlman, "The Anti-social Network: Countering the Use of Online Social Networking Technologies by Foreign Terrorist Organizations," accessed January 21, 2012, http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20Kohlmann%5B1%5D.pdf.

The simplicity and effectiveness of this feature was manifested in the case of the five young Muslim men from the Washington, DC are, who were arrested in Sargodha, Pakistan in 2009. They attempted to join al-Qaida forces on the Afghan-Pakistani border. According to the police report, Taliban member, "Saifullah", recruited the five men. The recruiter contacted one of the men, Ahmed Abdullah Minni, who had "become a regular feature" on YouTube for commenting repeatedly on videos of attacks on American troops. His continuous praise and "online vitriol" grabbed the attention of the recruiter, who began contacting Minni.[62] This is just one of many cases in which online social network platforms have recruited and led to actual action.

Some critics have argued that the effectiveness of recruiting and propagandizing through online social networks is relatively low and has little impact. In a testimony before the House Subcommittee on Counterterrorism and Intelligence, William McCants, analyst for the Center for Naval Analyses, argued that the success of social media propaganda is low. Quoting an anonymous online recruiter for al-Qaida, he stated:

> The [recruiter] posited that if you post al-Qaeda propaganda to all of the mainstream websites, only 10% of the people will likely look at it. Of those, only 10% will like what they see. Of those, only 10% will embrace the idea of jihad. Of those, only 10% will seek martyrdom. By this reasoning, ten thousand people out of a population of one billion Muslims, or 0.00001%, would go fight for al-Qaeda and even fewer would carry out a suicide operation . . . it is difficult to say why some become active supporters . . . What we can say is that the vast majority of people who watch and read al-Qaeda propaganda will never act violently . . . [63]

Nevertheless, there have been several examples. It is difficult to quantify the influence of radical material online and its effect in recruiting because of the clandestine nature; however, several of these cases have proven this point. In 2010, it was reported that Colorado nursing student uprooted and moved to Europe to join a terrorist cell, a cell, which had a $100,000 bounty on the Swedish cartoonist who depicted the Prophet Mohammed as a dog. The cell reportedly "brainwashed" her and her son according to her family. She had

[62] Kohlman, "The Anti-social Network…"

[63] William McCants, "Subcommittee Hearing: 'Jihadist Use of Social Media – How to Prevent Terrorism and Preserve Innovation.' Testimony of William McCants," Committee on Homeland Security's Subcommittee on Countertorrism and Intelligence, accessed January 14, 2012, http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20McCants.pdf.

apparently formed a relationship with a radicalized Colorado man, Najibullah Zazi, who had pleaded guilty the earlier to a plot to blow up parts of a New York subway. The relationship was found and developed online. She was later arrested along with the American woman, "Jihad Jane," who also joined the cause after watching online lectures from the English-speaking Anwar al-Awlaki. She was also the woman, who had been very active in online forums and discussions on radical YouTube videos.[64]

In another case, a 30-year old Jordanian doctor, Humam al-Balawi, was recruited by both Jordanian and American intelligence to infiltrate al-Qaida's leadership in Afghanistan. The man did not have direct connections with al-Qaida, but had a "passion for the Internet." He was considered a benign "computer nerd but, instead had very serious intentions." With his online credentials, he established contacts within al-Qaida and the Taliban, and instead of acting as an informant for the intelligence agencies, he turned against them. This "seemingly quite family man" was "recruited and transformed into a terrorist" through his online engagement in online social networks. It was later discovered that Al-Balawi regularly posted on online forums and even interviewed for online propaganda magazines for al-Qaida and the Taliban. He even shared his intentions and plans to participate in the cause. He eventually volunteered to a suicide bombing at a base in Afghanistan, which ended up killing seven CIA agents.[65]

In 2010, Roshanara Choudry, made headlines in the U.K. when she stabbed British MP Stephen Timms for voting for the Iraq war. She did so out of revenge for the people of Iraq. She sought to be a martyr because "it was the best way die." She explained in interviews that she was motivated after listening to Yemeni-American cleric Anwar al-Awlaki's lectures online. Explaining how she found his lectures, she said, "On the Internet … if you go to YouTube, there's lots of his videos there and if you do a search they just come up … I wasn't searching for him, I just came across him … I used to watch videos that people used to put up about like how they became Muslims."[66] This example is one case

[64] "Terrorists Targeting Children via Facebook, Twitter," *Fox News*, March 15, 2010, http://www.foxnews.com/scitech/2010/03/15/terrorists-targeting-children-via-facebook-twitter/.

[65] Vergel, "Security Expert: Social Networking…"

[66] Kohlman, "The Anti-social Network…"

that counters the argument that only already radicalized individuals will seek out this material online. The prevalence of this information on mainstream sites like YouTube and Facebook inevitably come across the screens of impressionistic individuals and do play in role in radicalizing them.

In early 2012, a Maryland man and former U.S. Army soldier was arrested and charged with providing material support to the Somalian terrorist group, al-Shabaab. Craig Baxam converted to Islam after reading about a radicalized view of the religion online during the last months of his service in the military. After he left, he attempted to travel to Somalia, but was stopped by Kenyan officials, who found about $700 of cash intended for al-Shabaab. He admitted to FBI agents that he'd be a part of al-Shabaab once he reached Somalia and that he was "looking for dying with a gun in my hand."[67]

Flashpoint Global Partners, a security firm, has identified at least 120 individuals, including U.S. nationals, who have "graduated from being mere "pajama-hideen," those who participate in online jihad, to those taking an actual role in terrorist activity during the past seven years. Out of the 120, most have been killed in Predator drone strikes, failed bomb-making activities, and gun fights with "infidel" adversaries.[68] Though the numbers may appear relatively small, exploited social media does play a role in propagandizing and recruitment.

On the other hand, drug cartels use of these online platforms for slightly different propagandistic reasons. Their videos are used to intimidate other cartels, police, and anyone who is tenacious enough to blow the whistle. The videos often portray images of heavily armed men or taped executions to demonstrate a show of force.[69] More specifically, drug cartels have used YouTube to post videos of rival cartel members confessing to crimes, often after torture and under gunpoint; this is a form of propaganda and as a way of weakening its members.

[67] "FBI: Ex-Soldier Tried to Aid Terrorists," *CBS News*, January 9, 2012, http://www.cbsnews.com/8301-201_162-57355319/fbi-ex-soldier-tried-to-aid-terrorists/.

[68] Kohlman, "The Anti-social Network…"

[69] Nacha Cattan, "Mexico's Drug War Hits YouTube Against Rival Groups," *Christian Science Monitor*, November 5, 2010, http://www.csmonitor.com/World/Americas/2010/1105/How-Mexican-drug-gangs-use-YouTube-against-rival-groups.

For instance, in September of 2010, a YouTube video was posted showing two men, who confessed to murdering a group of Mexican tourists in Acapulco. They called it a revenge attack against the violent Michoacán-based cartel, La Familia. This led authorities to believe that the two men were held captive under La Familia members. The video also led authorities to a mass grave of 18 bodies. Not only did the video do damage to La Familia's rivals, but also sent out a message to others that it was in control, that it was the law, not the police. "This tactic is used not only to incriminate rival gangs, but also to discredit the authorities," says Jorge Chabat, who studies the drug war at the Center for Research and Teaching in Economics in Mexico City.[70]

Drug cartels want it two ways: "They want to censor the negative things that people say about them" online, but want "a forum to post their own propaganda, or have sympathizers do it on their behalf."[71] Nevertheless, cartels are exploiting social media for their own purposes and have made it a part of their propaganda efforts. They have also threatened the general public against using social media to comment on the cartels or provide information to authorities by brutally killing and dismembering men and women who have used social media to make counter-cartel comments.[72]

CYBERCRIME

There have been indications of cyber criminals colluding with terrorists and drug traffickers. The use of cybercrime by clandestine groups like terrorists and drug traffickers reveals the financial success of online credit card fraud and identity theft. As of 2009, cybercrime surpassed drug trafficking as the number one illegal moneymaker.[73] (Symantec).

[70] Cattan, "Mexico's Drug War Hits…"

[71] John Burnett, "Mexican Drug Cartels Now Menace Social Media," *NPR*, September 23, 2011, http://www.npr.org/2011/09/23/140745739/mexican-drug-cartels-now-menace-social-media.

[72] "Mexican Social Media Boom…"; NR Staff, "'Blogger's Beware'- Drug Cartel Mutilate Two Blogger's In Mexico!" *Naija Resource*, last modified September 16, 2011, http://www.naijapidginenglish.com/2011/09/16/bloggers-beware-drug-cartel-mutilate-two-bloggers-in-mexico/.; Emily Moore, "Killed for Tweeting - Mexican Cartel Drug Hangs Couple From Bridge as Warning After Torture," *Wish I Didn't Know*, last modified September 16, 2011. http://wishididntknowthat.tumblr.com/post/10290242074/killed-for-tweeting-mexican-cartel-drug-hangs.

[73] "Mexican Crime Groups Expand into Cyber World," Cyber Risk Report, *Cisco*, accessed September 22, 2011, http://www.cisco.com/web/about/security/intelligence/CRR_jun13-19.html.

The attractiveness of cybercrime (low-cost, simplicity, and anonymity) has invited nearly every underground group to exploit Internet users.

> Cybercrime has increased dramatically in past years, and several recent terrorist events appear to have been funded partially through online credit card fraud. Reports indicate that terrorists and extremists in the Middle East and South Asia may be increasingly collaborating with cybercriminals for the international movement of money, and for the smuggling of arms and illegal drugs. These links with hackers and cybercriminals may be examples of the terrorists' desire to continue to refine their computer skills, and the relationships forged through collaborative drug trafficking efforts may also provide terrorists with access to highly skilled computer programmers.[74]

In a 2010 House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security, Assistant Director, Gordon M. Snow testified that cyber criminals are using a variety of schemes to defraud social network site users. He discussed some of the schemes used by online attackers: social engineering, fraud schemes, phishing scams, and data mining.[75]

As previously mentioned, online social networks make impersonating and creating new identities simple. Online social engineering is a derivative of one of the oldest forms of deception. These are basic online confidence or "con" men, who convince trusting Internet users to give them access to their personal information.[76] Social network sites have facilitated social engineering by providing personal information on potential victims.

One technique used by criminals is a creation of "dummy" or fake social network accounts and then generating thousands of "friend" requests. "If accepted, not only can the attacker target that 'friend' directly, but he or she can also target the victim's list of friends."[77] Lists of friends on SNS easily increase the amount of potential cybercrime victims.

[74] John Rollins and Clay Wilson, "Terrorist Capabilities for Cyberattack: Overview and Policy Issues," CRS Report for Congress, last modified January 22, 2007, http://www.fas.org/sgp/crs/terror/RL33123.pdf.

[75] Gordon M. Snow, "Statement of Gordon M. Snow Assistant Director, Cyber Division Federal Bureau of Investigations Before the House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security," last modified July 28, 2010, http://judiciary.house.gov/hearings/pdf/Snow100728.pdf.

[76] Ibid.

[77] "Symantec Report on Attack Kits and Malicious Websites," *Symantec*, accessed April 3, 2011, https://scm.symantec.com/resources/b-symantec_report_on_attack_kits_and_malicious_websites_21169171_WP.en-us.pdf.

Frequently, the attacker will employ the use of false profiles of celebrities, attractive women, or cartoons. These types of profiles are more likely to be accepted by strangers. In a 2011 survey, one out of every five men admitted to accepting friend requests from women even if they were complete strangers.[78]

Fraud schemes employing social network sites are extremely common. One example includes a fraudster gaining access to SNS account and sending messages to all of the user's friends seeking assistance. The fraudster claims to be the friend, trapped in a foreign country, typically a victim of robbery, and now without financial means. The attacker will then ask the friends to wire money to an overseas account. Often, concerned friends will wire money without validating the account and will later discover they were scammed.[79]

Phishing is another form of social engineering in which an attacker attempts to fraudulently obtain sensitive information from "a victim by impersonating a trustworthy third party."[80] An example, a phisher would misrepresent himself or herself as a well-known company or charity and would ask individuals for personal or financial information via email. The emails are sent out en masse are not targeted to a certain individual or group.

Spear-phishing is different in that it does target a specific individual or group; it does not spam non-discriminately. Spear-phishers have usually conducted research on their victim through the use of social networking sites or by other means. They focus on a subgroup of people or individuals. A spear phish will look official and appear to come from a legitimate source. For example, an email would appear to be from an executive of the company or a systems administrator asking for login IDs and passwords.[81]

Snow stated that cyber criminals also use data mining on social network sites in order to "extract sensitive information about their victims." This can happen on either a small or large scale. An example he shared was the use of online "get-to-know-you" quizzes sent out

[78] Bob Sullivan, "Would you 'friend' a stranger?" *MSNBC*, March 22, 2011, http://redtape.msnbc.msn.com/_news/2011/03/22/6501983-would-you-friend-a-total-stranger.

[79] Snow, "Statement of Gordon M. Snow…"

[80] Tom Jagatic, Nathaniel Johnson, Markus Jakobsson, and Filippo Menczer, "Social Phishing," School of Informatics, *Indiana University, Bloomington*, last modified December 12, 2005, http://www.indiana.edu/~phishing/social-network-experiment/phishing-preprint.pdf.

[81] Stephen Northcutt, "Spear Phishing," Security Laboratory, *SANS Institute*, last modified May 9, 2007, http://www.sans.edu/research/security-laboratory/article/spear-phish.

on sites such as Facebook, which ask seemingly harmless questions. However, the questions are usually the same or similar questions online financial sites, email services, and social network sites will ask the user to answer in order to access the account or change the password.[82]

As funds dry up from traditional donors and nation-states, terrorists and their sympathizers have turned to anonymous online cybercrime and fraud. In 2007, three British residents and terrorist-sympathizers were sentenced for using the Internet to incite murder. The men used stolen credit card information and online stores to purchase items for "fellow jihadists in the field—night vision goggles, tents, global positioning satellite devices, prepaid cell phones, plane tickets. They also used stolen credit cards to register web domains and servers. In total, they charged over 3.7 million dollars from a database of 37,000 stolen credit numbers.[83]

In another case reported by the FBI, a terrorist cell in Spain with ties to al-Qaida "used stolen credit cards for logistical items for the cell."[84] Additionally, in a report from the House Homeland Security Committee, FBI officials indicated that Al Qaeda had used identity theft and credit card fraud to support terrorist activities; moreover, according to press reports, Indonesian police officials believed that a 2002 bombing in Bali was partially financed through online credit card fraud."[85]

In a CRS Report on terrorist cybercrime activity, John Rollins stated:

> Cybercrime has increased dramatically in past years, and several recent terrorist events appear to have been funded partially through online credit card fraud. Reports indicate that terrorists and extremists in the Middle East and South Asia may be increasingly collaborating with cybercriminals for the international movement of money, and for the smuggling of arms and illegal drugs. These links with hackers and cybercriminals may be examples of the terrorists' desire to

[82] Snow, "Statement of Gordon M. Snow…"

[83] Clay Wilson, "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress," CRS Report for Congress, last modified January 29, 2008, http://www.fas.org/sgp/crs/terror/RL32114.pdf.

[84] United Nations Counter-Terrorism Implementation Task Force, "Countering The Use Of The Internet for Terrorist Purposes-Legal and Technical Aspects," CTITF Working Group Compendium, accessed March 4, 2012, http://www.un.org/es/terrorism/ctitf/pdfs/ctitf_interagency_wg_compendium_legal_technical_aspects_web.pdf.

[85] Wilson, "Botnets, Cybercrime, and Cyberterrorism…"

> continue to refine their computer skills, and the relationships forged through collaborative drug trafficking efforts may also provide terrorists with access to highly skilled computer programmers.[86]

A specific case in 2005, which displayed al-Qaida's computer hacking and cyber crime skills, involved an al Qaida Internet hacker, who called himself "Irhabi---Terrorist---007." He was instrumental in hacking into web servers and sites to post propaganda for the Iraqi insurgents led by Abu Musad al-Zarqawi. He was also known for teaching hacking skills to other online jihadists and how they could use their skills to further their cause. In a *Washington Post* article, it reported that Irhabi 007 was a "master" in "hacking, programming, executing online attacks, and mastering digital and media design."[87]

Intelligence services around the world searched for Irahbi 007's true identity for almost two years. The search ended when Scotland Yard arrested 22-year old Younis Tsouli in London for his involvement in a supposed bomb plot. When authorities arrested Tsouli, they were unaware of his online activity. It was only until investigators further probed that they discovered their luck. Tsouli was Irhabi 007. They also found stolen credit card information in his home. He had used the stolen information and cards to pay for servers on which to post jihadist propaganda.[88] This case is not only another example of cybercrime, but also an indication of terrorist groups' desire to increase its technical abilities online.

As mentioned previously, Symantec reported that cyber crime is now more lucrative than drug trafficking. As such, drug cartels have expanding into cyberspace, which is more lucrative, less costly, and safer than the "gun-toting urban warfare" associated with drug trafficking activities.[89]

In February 2011, the Mexican government released reports on the number of reported cyber crimes. The data indicated that in 2009 alone, the police handled over 1,400 cases of cyber crime. This did not include the countless number of unreported crimes. Of the crimes, fraud led as the number one online crime. Interpreting these numbers,

[86] Rollins and Wilson, "Terrorist Capabilities for Cyberattack…"

[87] Rita Katz and Michael Kern, "Terrorist 007, Exposed," *The Washington Post,* March 26, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/03/25/AR2006032500020.html.

[88] Ibid.

[89] "Mexican Crime Groups Expand…"

IntelliShield interpreted that the rising number of cyber crimes could be attributed to drug cartels moving over to “low cost/high impact” cyber crimes.[90]

Because drug cartel members usually lack the technical training and knowledge, there have been reports of computer savvy individuals being hired or held against their will to steal information online for credit card and identity fraud. According to a feature in a Mexican newspaper, Excelsior, Fernando Ernesto Villegas Alvarez, a 24-year old computer programmer in Mexico City was coerced to work for a drug lord, Edgar Valdez Villareal.[91]

Social network sites are making it more possible and easier for clandestine groups to participate in cyber crime. The large trove of personal information posted publicly or sometimes effortlessly extracted information has contributed to the rise of cyber crimes. U.S. Attorney Terrence Berg stated, “With millions of users packing these sites with personal information of every type, from family photos and movies to career interests to what used to pass for private gossip. . . these sites are gargantuan warehouses of valuable [information] that could be exploited if made accessible to those with criminal ends in mind.”[92]

SNS further enables the process of stealing personal information through social applications that leave accounts vulnerable by viruses. For example, daily Facebook accounts are hacked into through means of deceptive links. If the victim plays the website’s games and uses the Facebook Credits, their credit card information is stored and readily available to be stolen. Groups such as terrorists or drug cartels have recognized its effectiveness and have thus exploited SNS for their own financial gain, which is in addition to the other benefits SNS provide.

Most alarming is the growing potential and sheer simplicity of information theft. Free programs, such as Firesheep, allow users to view and access the web browsers of those sharing the same open wireless Internet network. If the user is not utilizing the secure browsing setting (https) on Facebook for example, the Firesheep user can easily access the

[90] “Mexican Crime Groups Expand…”

[91] Ronan Graham, “Are Mexico Drug Gangs Drafting Hackers?” *Borderland*, last modified July 18, 2011, http://www.borderlandbeat.com/2011/07/are-mexico-drug-gangs-drafting-hackers.html.

[92] Nathan Petrashek, "The Fourth Amendment and the Brave New World of Online Social Networking," *Marquette Law Review* 93, no. 4 (2010): 1-36, http://scholarship.law.marquette.edu/cgi/viewcontent.cgi?article=5029&context=mulr.

unknowing victim's Facebook account and collect both personal and financial information. While most bank websites and email services are protected against Firesheep, Twitter and other similar SNS are easily accessible through this program.

Moreover, geo-locating social network sites such as Foursquare, Facebook, and Twitter, provide an idea of where its users spend their time. A cyber criminal could notice that an individual frequently spends their time at a certain Starbuck's café for example, where they use their smart phone or laptop and update onto Foursquare. Now the cyber criminal has easy access to the individual's personal information and potentially even their financial information using software like Firesheep. This opens up online credit card and identity theft to anyone, regardless of an individual's technical abilities.

FUNDRAISING AND MONEY LAUNDERING

In a 2010 article entitled, "Terrorist Financing and the Internet," Michael Jacobson, stated, "Technology and globalization have . . . enabled small groups of alienated people not only to connect but to raise resources for attacks without need for an established terrorist organization."[93] Coupled with the advancement of technology, the crackdown on bank accounts in the United States after 9/11 may have contributed to the migration of money transfers from traditional means to online transactions. Many online payment systems are unregulated by international regulations and are as a result often difficult to detect.

In a U.N. report, the members of the CTIFT expressed concerns over the different systems of money transfer and laundering online. The Internet in general provides limitless means for terrorists to transfer and hide money. For example, there have been reports that terrorists have used online gambling sites to launder money. Terrorists have also used a variety of techniques from which to raise money online through e-commerce: selling CDs, DVDs, T-shirts and other paraphernalia. They have even employed the simple and straightforward method of "accepting donations" on their websites or blogs using electronic bank transfers or electronic payment methods such as PayPal.[94]

[93] Jacobson, Michael, "Terrorist Financing and the Internet," *Studies in Conflict & Terrorism* 33, no. 4 (2010): 353-363.

[94] United Nations Counter-Terrorism Implementation Task Force, "Countering the Use of the Internet…"

These groups also create front “charitable organizations” through which funds are raised. Unbeknownst to the donator, instead of funding a genuine Muslim charity, they are in fact funding an extremist group.[95] The Paris-based Financial Action Task Force stated, “the misuse of non-profit organizations for the financing of terrorism is coming to be recognized as a crucial weak point in the global struggle to stop such funding at its source.” There have been several cases of terrorist-operated charities putting up websites and soliciting donations under the guise of actual humanitarian assistance.[96]

For instance, the Global Relief Foundation (GRF), which was later discovered as a front charity organization for al-Qaida and the Taliban, set up a website seeking donations. The website described its group was “organized exclusively for charitable, religious, education, and scientific purposes.” Its mission statement included its supposed “work in emergency relief, medical aid, advancement of education and development of social welfare . . . [acting] with goodwill towards all people.”[97]

Reports of specific cases of fundraising and money laundering through social network sites are limited; however, the CTIFT reported that social media sites such as Facebook, YouTube, and MySpace have “[allowed] charities to raise and solicit funds via [these] sites.” The report also noted, “Several terrorist organizations are already using social networking applications as the latest method for raising money for their activities.”[98] The CTIFT also noted the adoption of cellular telephone applications (apps) by charitable organizations, which are available as “downloads or as plug-ins for social networking sites.” The CTIFT’s concern derives from the fact that terrorists’ fundraising through bogus charitable organizations online will extend into social network sites and phone apps. These transactions would be even more difficult for government officials to track.[99]

The potential of money transfers online is limitless. Facebook’s Marketplace, which is similar to an online garage sale, has the potential of more money laundering and money

[95] United Nations Counter-Terrorism Implementation Task Force, “Countering the Use of the Internet…”

[96] Jacobson, “Terrorist Financing and the Internet”

[97] Ibid.

[98] United Nations Counter-Terrorism Implementation Task Force, “Countering the Use of the Internet…”

[99] Ibid.

transfers. For instance, a member of a clandestine group could post a bogus posting of an item like a vehicle for sale and wait for their recipient to supposedly purchase the item. This provides an opportunity for groups to transfer small amounts of money. Many transfers of small amounts can easily add up to significant amounts of money, particularly if the transactions are done via underground banking systems such as the hawallah system that is really transferring "credits" rather than actual cash.[100]

The House hearings on Second Life as discussed previously, also raised the question of whether terrorists could potentially exploit the site for money laundering or fundraising purposes. The virtual world uses currency called Linden dollars, which can be exchanged for US dollars and visa versa. Users can purchase everything from virtual real estate to apparel for the user's avatar. Government officials became concerned that the money transactions occurring in Second Life would provide an opportunity for terrorists to launder and transfer money. Nevertheless, Linden Labs, the creators, argued that it monitors financial exchanges and most users only withdrawal an average of one US dollar at a time; large transactions would be easily spotted.[101]

As social media sites evolve and further connect users' financial activities to their SNS accounts, further opportunities for clandestine groups to transfer and launder money will arise. Government officials will have to make further efforts to keep up with the growing technologies in order to prevent further exploitation of social media for illegal financial transactions.

INTELLIGENCE GATHERING

According to the al-Qaida Handbook, terrorists are encouraged to search online for data regarding "Government personnel and all matters related to them (residence, work place, times of leaving and returning, children and places visited)."[102]   All this information is

[100] Billy Steel, "Money Laundering – Business Areas Prone to Money Laundering," *Billy's Money Laundering Information Website*, accessed March 2, 2012, http://www.laundryman.u-net.com/page9_bus_prone_ml.html.

[101] Sharon Weinberger, "Congress Freaks Out Over Second Life Terrorism," Danger Room. *Wired*, last modified April 4, 2008, http://www.wired.com/dangerroom/2008/04/second-life/.

[102] "OPSEC and Safe Social Networking," The Official Homepage of the United States Army, *United States Army*, accessed March 3, 2012. https://ia.signal.army.mil/SocialmediaandOPSECbrief1.pdf.

effortlessly discovered through the simple search of open source social media. The CTITF reported that SNS provided "significant intelligence to terrorists . . . [social media makes] it easy to find many targets of interest, such as the names of diplomats working at an embassy, as well as their pictures and those of their spouses and children."[103]

In a 2009 study conducted by the U.S. Air Force, 300 out of 500 MySpace profiles of Air Force members provided enough personal information on the social network site to leave them vulnerable to a cyber attack or blackmail. The study found that 60% of Air Force members on MySpace provided too much information.[104] Because of the vulnerability social media sites can create, government officials have sent out warnings and have trained personnel on proper operational security.[105] [106]

Since 2009, social network sites have evolved to include geo-locating features. In one incident, a U.S. Government official on a sensitive trip in Iraq created a security risk when he tweeted his locations and activities frequently.[107]

Al-Qaida has also used other cyber capabilities to collect intelligence through unauthorized means. In an article on terrorism in the information age, Magnus Ranstorp, reported that al-Qaida had successfully broken into an email account of a U.S. diplomat in the Middle East. They had also acquired his bank statements, allowing them to track his "location and movement."[108] They used easily accessible and available tools from the Internet to crack the diplomat's password. The availability of these types of tools and other more damaging tools should alarm security officials considering it allows anyone with basic knowledge of computers to illegally retrieve sensitive information and even cause major disruptions to computer networks.

[103] United Nations Counter-Terrorism Implementation Task Force, "Countering the Use of the Internet…"

[104] Yosef Lehrman, "The Weakest Link: The Risks Associated with Social Networking Websites," *Journal of Strategic Security 3*, no. 2 (2010): 63-72, http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1014&context=jss.

[105] "OSPEC and Safe Social Networking"

[106] United Nations Counter-Terrorism Implementation Task Force, "Countering the Use of the Internet…"

[107] "OSPEC and Safe Social Networking"

[108] Dorothy E. Denning, "A View of Cyberterrorism Five Years Later," Center on Terrorism and Irregular Warfare, *Naval Postgraduate School*, accessed January 3, 2012, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA484928&Location=U2&doc=GetTRDoc.pdf.

Another example of terrorists gathering intelligence from social media platforms was the 2008 terrorist attacks in Mumbai. The attackers utilized easily operable and accessible technologies such as GPS systems, satellite phones, and Internet phones. The well-coordinated and technologically advanced planning also utilized geo-locating platforms such as Google Earth to plan its attacks by studying the maps of their targets.[109] It was also speculated that the attackers were monitoring the Twitter feed of citizens reporting the events and possible that the attackers were sending out misinformation also. The Pakistani government indicated their concern over this problem when it asked all Mumbai tweets to halt for security reasons.[110]

As discussed previously, drug cartels have utilized sites such as Facebook to gather intelligence on its enemies and victims. In the example mentioned already, they search the profiles of prominent businessmen and politicians, find the names and faces of their family members, and in turn, use this information to abduct. Cartels are "monitoring Internet sites, blogs, phone calls, and the famous social networks on a daily basis" in order to monitor their threats.[111] Cartels are taking note of the social media material that incriminates them. In a country where most journalists have to "self-censor" or else risk being a target of drug lords, and where government officials often self-censor too, social media has been crucial as a source of news. Nevertheless, this has been deemed as a threat by cartels as they have made public examples of the tenacious social media reporters.

In one case, blogger "Rascatripas" attempted to expose the atrocities by the Los Zetas, a violent drug cartel. He was soon after murdered in order to send a message to any other blogger contemplating doing the same. The Zetas found his personal identity easily through his use of social media.[112]

[109] Jeremy Kahn, "Mumbai Attackers Use Sophisticated Technology," *The New York Times*, December 9, 2008, http://www.nytimes.com/2008/12/09/world/asia/09iht-attack.1.18517890.html.

[110] Alexander Wolfe, "Twitter in Controversial Spotlight Amid Mumbai Attacks," *Information Week*, last modified November 29, 2008, http://www.informationweek.com/news/global-cio/interviews/229209104.

[111] "Social Media Boom in Mexico Draws…"

[112] "Blogging and Social Networking Turn Deadly in Mexico," *Flip the Media*, last modified December 23, 2011, http://flipthemedia.com/2011/12/why-blogging-and-social-networking-in-mexico-can-turn-deadly/.

In another incident, a Mexican Twitter user, Marisol Macias Castro, was found decapitated after she had posted the criminal activities of local cartel members.[113] In September 2011, two mangled bodies hanging from a bridge in Nuevo Laredo, Mexico sent a message to online critics of Los Zetas. Next to the disturbingly tortured and disemboweled bodies was a sign that read: “This is going to happen to all of those posting funny things on the Internet … You better [expletive] pay attention. I’m about to get you.” In addition to other mutilations, the fingers were mutilated, most likely a symbolic threat: fingers are used to type.[114]

Not only have Mexican cartels used social media for counterintelligence purposes; moreover, they have used their assassinations as propaganda to prevent any whistle blowing activity online. Although cartels have attacked traditional journalists and media, these cases demonstrate a potential new trend of cartel violence against social media users.

Social media users have not taken these warnings lightly. One anonymous journalist stated, “There is no point in denouncing something on the Internet if the authorities aren’t going to do anything about it; you are only exposing yourself to more danger.”[115] Mexican cartels have effectively silenced local traditional media outlets and have moved on to silencing online social media sources. The combination of the cartels’ arsenal of technology-savvy members, whether hired or coerced, and the sheer simplicity of uncovering social media users’ real identities, stifles genuine news from being reported. Section 3 will discuss how we can affordably assist citizens to safely and anonymously post cartel and terrorist activity with the assistance of social media.

[113] Erika Angulo and Wilma Hernandez, “Mexican Journalist on Drug Lords: If They’re Going to Kill You, They’re Going to Kill You,” World Blog, *NBC News*, February 24, 2012, http://worldblog.msnbc.msn.com/_news/2012/02/24/10497924-mexican-journalist-on-drug-lords-if-theyre-going-to-kill-you-theyre-going-to-kill-you.

[114] Mariano Castillo, "Bodies Hanging from Bridge in Mexico are Warning for Social Media Users," World, *CNN*, September 14, 2011, http://articles.cnn.com/2011-09-14/world/mexico.violence_1_zetas-cartel-social-media-users-nuevo-laredo?_s=PM:WORLD.

[115] “Social Media Boom in Mexico Draws…”

CHAPTER 3

SOCIAL MEDIA, LAW ENFORCEMENT, AND INTELLIGENCE: PROBLEMS AND POTENTIAL SOLUTIONS

After discussing how groups such as Islamic terrorist groups and Mexican drug cartels exploit social media, this chapter will discuss how law enforcement and the intelligence community utilize social media for their own purposes. This chapter also includes the problems that government agencies encounter when applying social media into investigations and intelligence collection. Moreover, this chapter will provide potential solutions to these problems, while focusing on using free to low-cost technologies.

The news has revealed the increased role social media now plays in the law enforcement and intelligence communities. Richard Stiennon, chief research analyst with IT-Harvest stated, "Social media is changing how people organize and how sentiment is spread. For the [government] to tap into that is logical."[116] Most government agencies have recognized the importance and clout of social media. This is evident in several agencies and departments' interest and even application of social media monitoring. Although much of what occurs in the realm of intelligence gathering and homeland security issues remain mostly classified, the government has openly revealed some of its programs.

CENTRAL INTELLIGENCE AGENCY (CIA)

The Central Intelligence Agency (CIA) has already actively employed the use of social media monitoring on foreign nationals. Former CIA Director General Michael Hayden told a conference in 2008, "there's a real satisfaction in solving a problem or answering a

[116] Mello, John P. Jr., "FBI Looking to 'Friend' Terrorists," Cybersecurity, *Tech News World,* last modified January 30, 2012, http://www.technewsworld.com/rsstory/74295.html.

tough question with information that someone was dumb enough to leave out in the open."[117] According to a National Public Radio (NPR) broadcast in 2011, a group within the CIA actively monitors the activity of people overseas on popular SNS. The several hundred staffers of the Open Source Center are experts in searching open-source material, whether it is a radio broadcast or a tweet. The information collected is fed to U.S. policymakers to assist in decision-making. For instance, "what next step should they [policymakers] take, what might be the reaction, or the fallout on the ground."[118]

SNS provide useful and timely impressions of the general attitudes of people in foreign countries, something of which was more difficult to do prior to the age of popular SNS usage. The CIA claimed that the monitoring of SNS users abroad predicted events such as the "fallout from the revolt in Egypt," and the region-wide Arab Spring in 2011. Although the CIA could not predict precisely when and how quickly it would occur, the monitoring did provide an insight to intelligence officials of the volatile climate in the Middle East and the inevitable uprisings.[119]

It was reported in 2010 that CIA's contractor In-Q-Tel, which handles the intelligence community's data analysis, invested in the company Record Future, which its program "goes beyond search" by "looking at the invisible links" from thousands of websites and social media.[120] This investment is further evidence of the U.S. intelligence community's interest in social media monitoring and analysis.

Challenges arise for the CIA however in areas of the world where Internet network infrastructures are weak. As a result, the CIA is face with an additional problem of the "SMS phenomenon," where people use cell phones to go online and communicate. Doug Naquin, director of the CIA center, stated that this is occurring in less modernized countries such as Afghanistan and Pakistan, terrorist groups like the Taliban and al-Qaida set up closed

[117] Noah Shachtman, "Exclusive: Google, CIA Invest in 'Future' of Web Monitoring," Danger Room, *Wired*, last modified July 28, 2010, http://www.wired.com/dangerroom/2010/07/exclusive-google-cia/?utm_source=Contextly&utm_medium=RelatedLinks&utm_campaign=Previous.

[118] "How does the CIA use Social Media?" *NPR*, last modified November 7, 2011, http://www.npr.org/2011/11/07/142111403/how-does-the-cia-use-social-media.

[119] Ibid.

[120] "Exclusive: Google, CIA Invest in 'Future'…"

networks of subscribers, who receive “private” text messages with updates and operational intelligence. This in turn is a roadblock to the CIA since it would require NSA eavesdropping methods in order to penetrate the networks and retrieve information.[121] Problems like these reveal the limits each agency has when monitoring social media isolated from other agencies.

DEPARTMENT OF HOMELAND SECURITY (DHS)

The Department of Homeland Security (DHS) has also shown interest in social media and already actively monitors sites such as Twitter and Facebook. In a testimony before Congress, DHS officials, Mary Ellen Callhan and Richard Chavez, testified that the National Operations Center (NOC), which runs the program, “fulfill[s] its statutory responsibility to provide situational awareness and to assess the potential value of the public information within the social media realm” by examining social media sites in combination with traditional media sources. The department also uses the information operationally in “situations where particular programs within the Department or its components may need to access material on social media or individual profiles in support of authorized missions.”[122]

In January of 2012, DHS’s monitoring program attracted public attention when two British tourists were detained and denied entry into the U.S. after tweeting a joke about “digging up Marilyn Monroe” and planning to “destroy America.” What was thought to be a harmless joke (“destroy” is British slang for “partying”) was taken seriously by DHS, which had monitored Twitter and found the men to be a threat.[123] Civil liberties advocates and critics grew alarmed over the department’s monitoring program and believed it went too far.[124]

[121] “How does the CIA use…”

[122] Public Intelligence, “Video: DHS Testimony on Social Networking and Media Monitoring,” *Global Research*, last modified February 18, 2012, http://globalresearch.ca/index.php?context=va&aid=29369.

[123] Matthew Ingram, “Twitter Users Beware: Homeland Security Isn’t Laughing,” *Bloomberg Businessweek*, last modified January 30, 2012, http://www.businessweek.com/technology/twitter-users-beware-homeland-security-isnt-laughing-01302012.html

[124] Heather Callaghan, “British Tourists Arrested for Tweets of Terror,” *Activist Post*, last modified January 31, 2012, http://www.activistpost.com/2012/01/british-tourists-arrested-for-tweets-of.html.

The Twitter incident revealed how data-mining SNS can produce intelligence; however, it does reveal how the method has its limitations. Though DHS is prudent to utilize the open-source information, it must learn to filter and cross-reference the information on SNS with public records i.e. criminal records, immigration papers, etc. Otherwise, more time will be wasted on harmless individuals and furthermore, the overreactions will cause the public to distrust the government.[125]

DHS also uses social media to connect with the public. It utilizes Facebook and Twitter accounts in order to update the public on the department's activities and initiatives. It discusses issues from cybersecurity to tornados. Its Twitter profile has over 70,000 followers and its Facebook page has over 40,000. Additionally, FEMA has launched an application for smart phones that provides information on preparedness in different disaster situations. Moreover, the Transportation Security Administration (TSA) has also launched a mobile application, "MyTSA Mobile Application," which provides the public with relevant travel information such as security checkpoints.[126]

The majority of NSA's social media activity remains speculative. Under the assumption that NSA is collecting and sifting through cellular phone calls, Internet searches, visited websites, and emails, it is somewhat safe to assume that the NSA is also gathering information through social media. Moreover, with its capabilities, it is also possible that the NSA could go beyond open public data derived from social media and extract data from private messages, private profiles, and other private information.[127] The limitations the CIA has faced such as the "SMS Phenomenon" are easily overcome with NSA's capabilities and technologies. This is the reason why several domestic agencies such as the Justice, Homeland, and Treasury departments send information they have obtained through their own surveillance programs to the NSA to analyze. NSA's sophisticated software sifts through the largesse of data and finds patterns that could be related to a terror suspect or other threats to national security. This social network analysis software causes critics to believe the data

[125] Ingram, "Twitter Users Beware…"

[126] Public Intelligence, "Video: DHS Testimony…"

[127] Siobhan Gorman, "NSA's Domestic Spying Grows as Agency Sweeps Up Data," *The Wall Street Journal*, March 10, 2008, http://online.wsj.com/article/SB120511973377523845.html.

mining is extending into social media.[128] Moreover, there have been supporting reports that the NSA has funded research "intended to develop its capability to 'harvest' massive amounts of social networking information."[129] Whether their assumptions are correct or not, it would be uncharacteristic for the NSA to ignore the vast amounts of open source data available for their analyses.

FEDERAL BUREAU OF INVESTIGATION (FBI)

What the FBI is currently doing with social media has not been publicly disclosed. What is known is that the law enforcement agency has subpoenaed and court ordered companies like Facebook, Twitter, and Google for user information. A Reuters review of the Westlaw legal database demonstrated that between 2008 and 2011, federal judges authorized at least two dozen warrants to search Facebook accounts. The FBI was included in the list of agencies, which requested the warrants. The cases dealt with acts of terrorism and other crimes. In general, these warrants allow law enforcement to "scour the accounts, delving into everything from friend's list, calendars, events, posting updates, links, videos, photos, and [even] rejected friend requests."[130]

In addition to these warrants, the FBI can also employ secret subpoenas and court orders. The Bureau's secret subpoenaing was placed in the spotlight when Twitter challenged the gag order that prevented Twitter from informing its users that the FBI searched their accounts. (This legal battle will be expounded upon in Chapter 4).

What we also know is that the FBI is openly searching for a new social media monitoring application, which would help search "publicly available" sources like Facebook and Twitter for national security purposes. In their request, the FBI is seeking an application that would have the ability to:

[128] Jon Stokes, "EFF's New Lawsuit, and How the NSA is Into Social Networking," Law & Disorder / Civilization & Discontents, *Ars Technica*, last modified July 23, 2009, http://arstechnica.com/tech-policy/news/2009/07/effs-new-lawsuit-and-how-the-nsa-is-into-social-networking.ars.

[129] Petrashek, "The Fourth Amendment and the Brave New World…"

[130] Ruth Manuel-Logan, "Facebook Warrants by Law Enforcement Agencies Surge," *All Facebook*, last modified July 13, 2011, http://www.allfacebook.com/facebook-warrants-by-law-enforcement-agencies-surge-2011-07.

- Provide "instant notifications of breaking events, incidents, and emerging threats that have been vetted and meet the defined search perimeters."
- Immediately access geospatial maps" that plot "US Domestic terrorist data"; "global terrorist data"; "US Embassy, consulate and military installations around the world"; weather conditions and forecasts; and "video feeds from traffic cameras."
- Immediately translate into English, tweets and any other open forum publicly available social media captured in a foreign language."
- "Instantly search and monitor key words and strings in all 'publicly available' tweets and any other 'publicly available social network sites/forums."
- "Geo-locate the open-source media social media 'search' by setting a radius by both miles and kilometers that will allow the user to quickly narrow the search to a specific area/region/location."
- "Geospatially locate bad actors or groups and analyze their movements, vulnerabilities, limitations, and possible adverse actions"[131, 132]

The FBI's request has also sparked controversy among civil and privacy rights groups. The legal implications will also be examined in chapter 4.

The FBI has also used its Facebook and Twitter to better connect with the public and to seek assistance from it. The FBI uses its Facebook and Twitter accounts to make citizens aware of its criminal cases, post wanted persons' pictures, ask for further information, and provide general tips for the public (cyber security tips, fraud scams, etc.).

In a February 2012 theft and murder case, the FBI used its social media accounts to post digital Wanted posters of Kenneth John Konias, Jr. to seek help from the public. The link was shared 487 times and received 140 comments from the community. Although the investigation is still continuing, the public involvement and reaction during this case demonstrates the clout of social media word-of-mouth and the important role it can play in investigations.[133, 134]

[131] Christina Warren, "Revealed: The FBI Wants to Monitor Social Media," U.S. and World, *Mashable*, last modified January 26, 2012. http://mashable.com/2012/01/26/fbi-social-media-monitoring/.

[132] "Social Media Application." *FedBizOpps*, last modified February 14, 2012, https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=c65777356334dab8685984fa74bfd636&_cview=1.

[133] Joann Pan, "FBI Uses Social Media to Catch Murder Suspect Who Stole $2.3 Million [VIDEO]," Social Media, *Mashable*, last modified March 9, 2012, http://mashable.com/2012/03/09/kenneth-konias-wanted-fugitive/.

[134] Federal Bureau of Investigation's Facebook page, accessed March 10, 2012, www.facebook.com/fbi.

DRUG ENFORCEMENT ADMINISTRATION (DEA)

The media has not extensively reported The Drug Enforcement Agency's (DEA) usage of social media in comparison to other government entities. However, similar to most law enforcement agencies, the DEA trains its agents and analysts to utilize social media in their respective investigations. In an unclassified public release of a training presentation given to DEA employees on the use of social networking sites in investigations, we discover some of the DEA's social media implementation practices are apparent. The presentation explains that SNS are subpoenaed and court ordered in a similar fashion to telephone and cellular service providers. The presentation explains that subscriber information (name, email address, physical address), payment methods, connection logs, and sometimes private content can be subpoenaed and court ordered. This demonstrates that the DEA is also subpoenaing and using court orders to obtain personal information from SNS providers.[135]

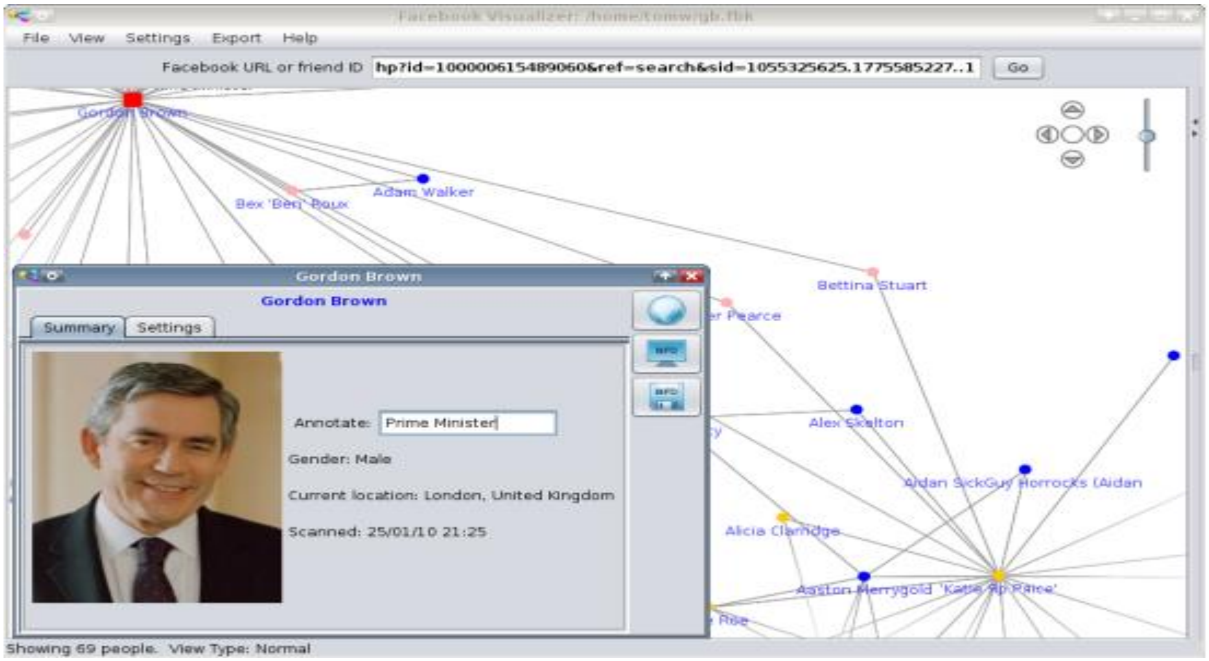
The training also teaches how to use an inexpensive network mapping and visualizing software called, Lococitato. The software mines publicly available information and creates maps of SNS users for sites such as Facebook, MySpace, and YouTube. Software for Facebook visualization is only available to law enforcement, but the other site visualizations are available to anyone willing to pay the fee. The software combs through data on a website and maps out a web of associations. Figure 2 is an example of Gordon Brown's Facebook network of friends.[136]

As demonstrated, the software has mapped former U.K. Prime Minister Gordon Brown's network of friends and associates on Facebook. This software can be utilized to discover the associates of suspects in investigations. Although some connections may appear non-germane, this type of visual information also produces invaluable intelligence that would not have been discerned with human analysis.

While the DEA is in the same Department of Justice as the FBI, there have been no public signs of it seeking for or adopting social media monitoring applications reminiscent to

[135] "Case Number: 10-0166-F," Drug Enforcement Administration, accessed February 22, 2012. https://www.eff.org/sites/default/files/filenode/social_network/20100514_dea_socialnetworking.pdf

[136] "Loco citato. Mapping Social Networks," *Lococitato*, accessed February 2, 2012, http://www.lococitato.com/.Ibid.



Facebook URL or friend ID hp?id=100000615489060&ref=search&sid=1055325625.1775585227..1

Gordon Brown

Annotate: Prime Minister

Gender: Male

Current location: London, United Kingdom

Scanned: 25/01/10 21:25

Showing 69 people. View Type: Normal

Figure 2. Facebook network visualization map. Source: Lococitato. "Loco citato. Mapping Social Networks." Accessed February 2, 2012. http://www.lococitato.com/.

the FBI's. The lack of cooperation and coordination between two federal law enforcement agencies within the same department, introduces a set of problems facing effective social media applications, which will be examined later in this chapter.

PROBLEMS FACING LAW ENFORCEMENT AND INTELLIGENCE OFFICIALS IN EFFECTIVELY UTILIZING SOCIAL MEDIA

Although these communities have made strides in adopting social media in their arsenal of investigation and intelligence gathering tools, changes should be made, more can be done to make the process more efficient, accurate, and simplified. In discussing recommended changes, the following section will include the underlying problems facing government agencies in fully utilizing social media and how these problems can be addressed.

Lack of Cooperation and Coordination

One existing problem is the lack of uniformity, cooperation, and coordination among law enforcement and intelligence agencies. There are sixteen different agencies alone in the American intelligence community. The duplicity is intended to create competition among the agencies and also put a system of checks and balances into place; however, critics see the duplication as government waste. Nevertheless, this system is intended to create better intelligence compared to a unitary system.[137]

The terrorist attacks on September 11, 2001 stirred debate on the intelligence community's effectiveness. The September 11th commission criticized that the intelligence community failed to "connect the dots." "Turf battles and inertia" surely contributed to the tactical failures of preventing 9/11, but the failures were indeed structural. The former structure served the country well during the Cold War, but hindered cooperation among members of the intelligence community as seen in the lack of information sharing between the CIA and FBI leading up to 9/11. They "sat astride the fundamental distinctions of the cold war" between intelligence and law enforcement, between foreign and domestic, and between public and private."[138]

Agencies such as the CIA and FBI have long approached homeland security from different worlds. CIA and its intelligence endeavors are "oriented toward the future and toward policy" while on the other hand, FBI's law enforcement is reactionary and focused on prosecution and not policy.[139]

Prior to the reforms resulting from the 9/11 Commission, there was a clear divide between "domestic intelligence" and "foreign intelligence." The divide was rooted in President Harry Truman's concern over giving the FBI the intelligence mandate; he was concerned it would risk creating a "Gestapo-like" organization. As a result, the intelligence mandate and foreign operations went to the Central Intelligence Group, the CIA's predecessor, and then to the CIA. Nevertheless, the CIG and CIA were and have been prohibited from law enforcement and domestic intelligence gathering.[140]

Since 9/11, the strict line between domestic and foreign has become blurred. "Threats to the homeland posed by terrorist groups are national security threats, and

[137] Michael Turner, "Intelligence and Homeland Security"(lecture, San Diego State University, San Diego, CA, September 16, 2010).

[138] Gregory F. Treverton, "DHS's First Year: A Report Card: Intelligence Gathering, Analysis, and Sharing," accessed January 31, 2012, http://www.tcf.org:8080/Plone/publications/pdfs/pb451/2.intelligence.pdf.

[139] Ibid., p. 63.

[140] Ibid., p. 64.

intelligence collected outside the United States is often very relevant to the threat environment inside the United States and vice versa."[141] Unlike the CIA and FBI, terrorist groups have no limits as to where they will plan and act, which calls for greater coordination within the intelligence community. The intelligence community must "do a better job of 'connecting the dots' of information from abroad and at home to produce more sophisticated assessments of the terrorist threat."[142]

The issues, which sprung from structural conditions, have also affected the coordination on social media efforts among the agencies within the intelligence community. While it is true that each agency has its own purpose, mission, and budget, each agency is forced to reinvent the wheel when it seeks to create a social media monitoring application. As aforementioned, the FBI is currently seeking the help of the private sector in building a social media monitoring application. It is intriguing that the FBI has not sought advice from agencies like DHS or the CIA, who already have adopted social media monitoring programs. Instead of the wastefulness of each agency building and creating an application, all relevant agencies could collectively budget for one uniform system that could be adapted to each agencies' purpose and jurisdictions (i.e. CIA could only monitor foreign nationals and not Americans). The streamlining would make intelligence sharing simpler and thus more common.

The intelligence community has utilized INTELINK, which is an internal government social network that employs social media software similar to Wikipedia and YouTube. This system allows intelligence sharing to more easily occur. Apparently, the system allows "different but connected systems at various levels of security classification" to operate. This unified system should be promoted in all agencies within the intelligence community and should lead into a smoother transfer of social media intelligence sharing. Though there have been vast improvements, more could be done to streamline and cut back on government waste.[143]

[141] Mark A. Randol, "Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches," Congressional Research Service, last modified January 14, 2009, http://www.fas.org/sgp/crs/intel/RL33616.pdf.

[142] Treverton, "DHS's First Year: A Report Card…," p. 64.

[143] Mark Drapeau and Linton Wells II., "Social Software and National Security: An Initial Assessment,"

Low Public Trust and Cooperation

Another considerable problem facing law enforcement and intelligence agencies and their utilization of social media is the lack of trust from the public. The government needs public trust to be fully effective. Increased transparency would assist in achieving this, as would increased public involvement. "The relationship between [law enforcement] and [citizens] can often yield valuable information that can lead to the discovery of dangerous activity." The public's involvement is a necessity in homeland security.[144] What the intelligence and law enforcement community need are cooperating citizens, who will report suspicious activity and trust that the information will be appropriately used.

In an article written in the International Association of Chiefs of Police, Police Chief Billy Grogan of Dunwoody, Georgia outlined three reasons social media should be embraced by law enforcement: online social networks offer a "natural platform for extending community policing efforts," social media provides a platform for departments to post its accomplishments, and the "people are there."[145] These reasons also apply to federal law enforcement.

Several federal agencies have already adopted social media platforms into their public diplomacy. As mentioned previously, the FBI and DHS already utilize Twitter and Facebook to seek the help from citizens, but also share information. There have been other examples. The State Department has initiated its CO.NX effort as a part of its "digital diplomacy." The interactive website provides a "virtual space" for communications between the community, subject matter experts, leaders, and the State Department. The site includes interactive web and video chats. It also links to CO.NX's Twitter feed and Facebook page. The interactive

Center for Technology and National Security Policy, *National Defense University*, accessed September 23, 2011, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA497525.

[144] Victoria L. Fresenko, "Social Media Integration into State-operated Fusion Centers and Local Law Enforcement: Potential Uses and Challenges," *Naval Postgraduate School*, accessed February 22, 2012, http://www.hsdl.org/?view&did=11536.

[145] Wayne Hanson, "How Social Media is Changing Law Enforcement," Justice and Public Safety, *GovTech*, last modified December 2, 2011, http://www.govtech.com/public-safety/How-Social-Media-Is-Changing-Law-Enforcement.html.

interface was named by Information Week as one of the top Government social media initiatives for its efforts in connecting people around the world.[146]

In addition, the State Department has teamed up with the U.S. Embassy in Prague to sponsor a social media gaming contest to "test ways social media and open source data can be used to track terrorists and locate missing children."[147] The contest, which is called "Tag Challenge," will be played in seven different major cities inside and outside the U.S. It is the brainchild of graduate students from six different countries, who organized the game out of "curiosity and fun." Considering a law enforcement body is not hosting the game, the event is approachable and the prize money is certainly a motivation for citizens to get involved. The site states that the game will offer government officials insight to "whether and how social media can be used to accomplish a realistic, time-sensitive, international law goal. " Moreover, the creators intend to post the results and data from the event after its conclusion. The event will occur on March 31, 2012 and will provide a trove of data on public participation in a law enforcement/social media application.[148] This activity could be adopted by other agencies seeking increased participation from the community and the data that will come from this exercise will open up further opportunities for research.

Another approach to garnering public participation and encouraging inter-agency cooperation would involve holding exercises, which involved government entities, universities, private citizens, and companies. In an exercise conducted at San Diego State University's Immersive Visualization Lab (Viz Lab), called Exercise 24 Mexico (X24), the usage of social media in a natural disaster scenario was explored. X24 Mexico was the third virtual exercise conducted at the Viz Lab, which utilized social media, "off-the-shelf" technologies, online tools, and crowdsourcing to building situational awareness in order to assist victims in natural disaster situations. Participants included the DHS Office of Health Affairs, NORAD-NORTHCOMM, US Customs and Border Protection/Global Borders College, Mexican Army and Navy, Mexico Federal Police, San Diego State University

[146] "IIP CO.NX. Online Destination for Global Digital Diplomacy," *IIP State*, accessed February 7, 2012, http://conx.state.gov/.

[147] Alissa Skelton, "U.S. Wants you to Test Terrorist Tracking with Social Media Game," U.S. and World, *Mashable,* last modified February 9, 2012, http://mashable.com/2012/02/09/social-media-tracks-terrorists/.

[148] Ibid.

Homeland Security program students, and even officials from Vietnam, India, and Somalia. Although the exercise was intended for a natural disaster case, my research explored its application to law enforcement and intelligence gathering.[149]

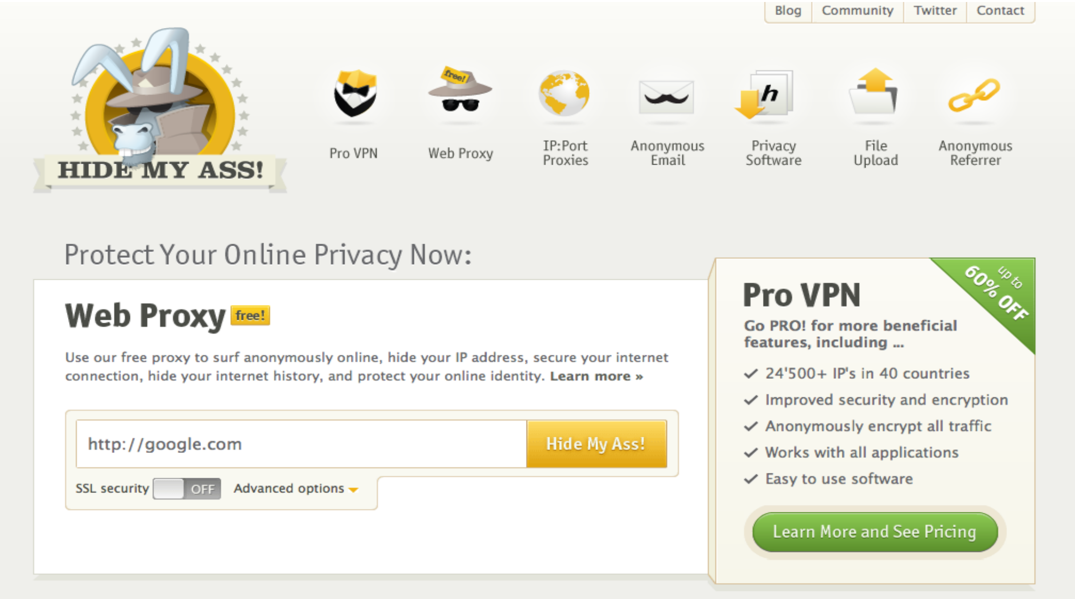
As this author participated in the Twitter injects and monitored the social media activity regarding our exercise, a major effort was undertaken to solve a problem facing Mexican SNS users. As aforementioned in Chapter 2, drug cartels have begun executing bloggers and SNS users for posting material online regarding the cartels' illicit activities. Although those who posted the material expected anonymity from the respective social media platforms, the cartels easily discovered their IP addresses and true identities. The murders of these bloggers have sent a chilling effect across Mexico. Citizens and journalists are afraid to report the violence and activity of ruling drug cartels. This greatly discourages citizens who want to know which locations to avoid or general news knowing it is not being reported through traditional media.[150] Moreover, without the tweets and blog posts from brave citizens, the U.S.'s own struggle in the drug war is deprived of valuable intelligence.

In order to address this problem, x24 sought to use a free to low-cost manner in which a citizen could anonymously tweet, ensuring that IP addresses and Twitter usernames would not be exposed. An evolving solution involves two simple low-cost technologies: the usage of a "Secret Tweet" account which post tweets anonymously and a proxy server, which would protect the users' IP addresses and locations. The site would most likely be trusted and utilized if it were not sponsored by a government entity, as many citizens in Mexico do not trust government officials. However, it would succeed if a non-profit group that had ties with trusted online community groups in Mexico sponsored the service. Although both sites were tested during the exercise and several flaws were found, several ways to address the flaws were also discovered. If more technical expertise and resources were available, numerous solutions to this need for anonymous tweeting and social media usage should be possible to develop.

[149] "Exercise 24," Viz Center, *San Diego State University*, last modified September 24, 2010, http://vizcenter.net/events/exercise-24/.

[150] "Blogging and Social Networking Turn Deadly…"

One solution was to essentially pull up a website for a proxy server---inserting this "man-in-the-middle" to protect the identity of the original sender. The intent was to use a service that did not require downloading or fees so there was as little digital trace as possible for the transaction. One such site is the website "HideMyAss.com." The website allows the user to put in any Internet address and anonymously access it by hiding the user's actual IP address, while at the same time securing the Internet connection and online identity. Figure 3 displays this site.



Protect Your Online Privacy Now:

Web Proxy free!

Use our free proxy to surf anonymously online, hide your IP address, secure your internet connection, hide your internet history, and protect your online identity. Learn more »

http://google.com

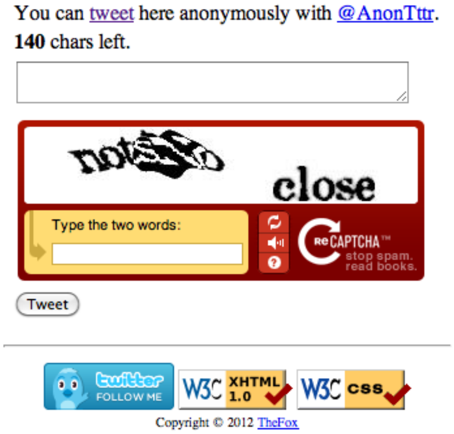
Pro VPN

Go PRO! for more beneficial features, including ...

- ✓ 24'500+ IP's in 40 countries
- ✓ Improved security and encryption
- ✓ Anonymously encrypt all traffic
- ✓ Works with all applications
- ✓ Easy to use software

Figure 3. Web proxy. Source: HideMyAss. "Hide My Ass! Free Proxy and Privacy Tools – Surf the Web Anonymously." Accessed January 31, 2012. http://hidemyass.com/.

Another solution was to access an anonymous tweeting service through the web proxy website. Please note Figure 3. During the exercise the author accessed www.secretweet.com; however, since the exercise, the website has since been down. With technical maintenance and filtering, a similar site providing this service could avoid technical issues. Nevertheless, the user would dictate their tweet in a text box as seen in Figure 4. The tweet will then go through an automated filtered or human filtering system, which will ensure the message's relevancy and ensure it is not spam.

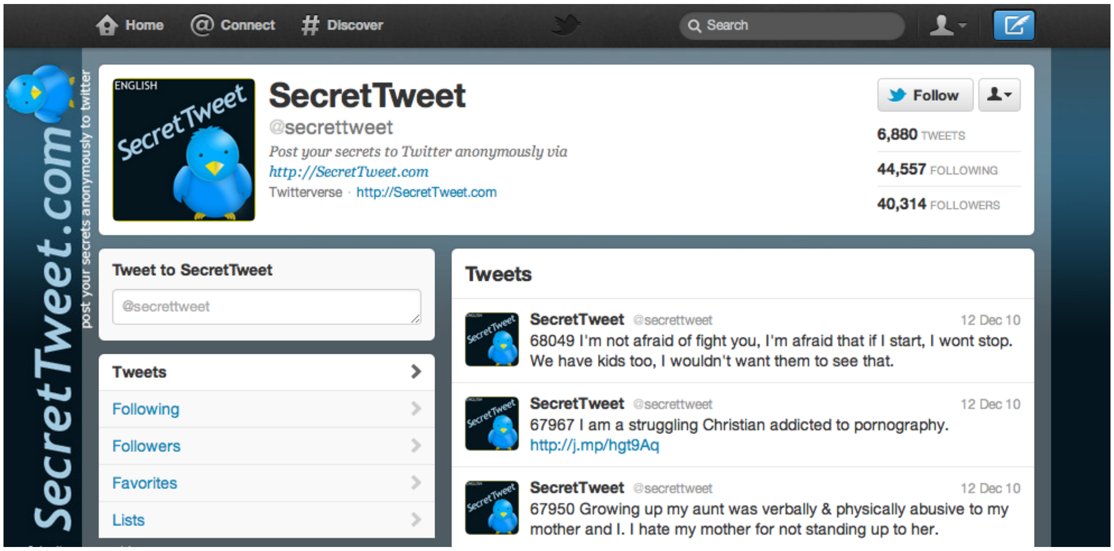


You can tweet here anonymously with @AnonTtr.
140 chars left.

Copyright © 2012 TheFox

Figure 4. Anonymous Twitter. Source: AnonTwttr. "Tweet Anonymously." Accessed March 9, 2012. http://anontwttr.fox21.at/.

After the tweet is approved, it is posted to the Twitter page shown in Figure 5, which will not reveal usernames, but will look similar to SecretTweet. These tweets on the webpage would be available to anyone (the public and law enforcement agencies); nevertheless, the use of a proxy server and anonymous tweeting service would protect the user.



SecretTweet
@secrettweet
Post your secrets to Twitter anonymously via http://SecretTweet.com
Twitterverse · http://SecretTweet.com

6,880 TWEETS
44,557 FOLLOWING
40,314 FOLLOWERS

Tweet to SecretTweet
@secrettweet

Tweets

SecretTweet @secrettweet 12 Dec 10
68049 I'm not afraid of fight you, I'm afraid that if I start, I wont stop. We have kids too, I wouldn't want them to see that.

SecretTweet @secrettweet 12 Dec 10
67967 I am a struggling Christian addicted to pornography. http://j.mp/hgt9Aq

SecretTweet @secrettweet 12 Dec 10
67950 Growing up my aunt was verbally & physically abusive to my mother and I. I hate my mother for not standing up to her.

Figure 5. SecretTweet. Source: SecretTweet. "SecretTweet (secrettweet) on Twitter." Accessed January 31, 2012. http://twitter.com/secrettweet/.

In an ideal situation, the proxy server and anonymous tweeting sites would be combined instead of having to access several websites. An application could also be created for smart phones and could have added features for pictures, videos, and even geo-locating. This application of relatively low-cost Internet tools and platforms could provide a greater level of information to citizens and governments than what is currently available. Citizens could feel more secure reporting cartel activity. It is important to note that the anonymity of the users will be protected as long as the guardians to the site have effectively protected the site from online intruders. An online application such as this could be adopted for other scenarios and regions also, where individuals fear retribution from either criminal or government groups.

Exercise 24 could be even further tailored to the needs of intelligence gathering or investigation. The success of the first three X24 events could indeed transfer over. In place of a natural disaster scenario, the exercise could include a terrorist attack scenario or a criminal investigative case, depending on the audience. A university could host the event, which invited government agencies (federal, local, intelligence and law enforcement), contracting companies, and SNS companies. The real-time, interactive event would be similar to the Tag Challenge, but involve more complex scenarios with real intelligence and law enforcement actors. This could improve icy relations between SNS companies and government agencies by creating personal relationships and providing face time. This would also provide opportunities for the community to engage with government officials.

The adoption of more social media tools in fusion centers across the country could also erase the line between public and private, local and federal. The 9/11 Commission concluded that the lack of information sharing contributed to the failure of preventing the 9/11 attacks. As a result, many state and local governments took the initiative to create fusion centers. They did so to “address gaps in homeland security, terrorism, and law enforcement information sharing by the federal government and to provide a conduit of this information within the state.” The federal government has also taken interest in fusion centers. Although initially intended for greater cooperation in state/local settings, fusion centers can be generally seen as:

> A collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity. Fusion centers

> may include a range of federal, state, and local entities and collect and analyze information related to homeland security, terrorism, and law enforcement.[151]

Fusion centers are beneficial to both the Department of Homeland Security and to state and local authorities if used effectively. DHS outlined the benefits. Some of them include:

> Improved information flow from state and local entities to DHS, improved situation awareness, access to non-traditional information sources, improved information flow from DHS to state and local authorities, local participation in dialogue concerning threats.[152]

In 2010, Victoria L. Fresenko explored how social media technologies could be utilized to "bridge the gaps between the public and fusion centers in addition to how it could "foster communication and cooperation collaboration between public citizens and the local law enforcement."[153] She used three case studies of three separate state fusion centers, which all used social media at different levels. In several situations, the authorities at the fusion centers found social media useful; however, they also found it had its limitations and obstacles. Many fusion center budgets are not robust enough to maintain a staff that can consistently utilize social media. The size of constituency is also a factor in the level of success social media plays in a fusion center's area. The fusion centers with the fewer constituents typically communicated and interacted with the public with greater ease than those centers with a greater amount of constituents.[154]

In addition, fusion centers must adhere to privacy and administrative laws. The legal issues could arise considering fusion centers' "use of private sector data, the adoption of a more proactive approach and the collection of intelligence [even through social media] by fusion center staff and partners."[155] However, many fusion centers understand the need to

[151] "Federal Efforts Are Helping to Alleviate Some Challenges Encountered b State and Local Information Fusion Centers," Homeland Security, *U.S. GAO*, last modified October 30, 2007. http://www.gao.gov/assets/270/268516.pdf.

[152] John Rollins, "Fusion Centers: Issues and Options for Congress," CRS Report for Congress, last modified January 18, 2008, p. 6, http://www.fas.org/sgp/crs/intel/RL34070.pdf.

[153] Victoria L. Fresenko, "Social Media Integration into State-operated Fusion Centers and Local Law Enforcement: Potential Uses and Challenges," *Naval Postgraduate School*, accessed February 22, 2012, http://www.hsdl.org/?view&did=11536 Accessed 22 February 2012.

[154] Ibid., p. 51.

[155] Rollins, "Fusion Centers: Issues and Options…," p. 12.

protect the privacy and civil liberties of its citizens. Several have created governing boards to oversee any potential violations. Some have even have policies that have been reviewed by the ACLU and other civil liberties organizations.[156]

Regardless of these obstacles, Fresenko found in her case studies that although the adoption of social media into fusion centers will initially be difficult, “the potential benefits of citizen collaboration greatly outweigh initial integration challenges.” The utilization of social media will promote greater collaboration between federal, state, and local entities in addition to private citizens.[157] She concluded, stating, “Community involvement in homeland security can be fostered through the use of social media tools; homeland security and local law enforcement professionals should provide an avenue for the public to participate and share what could be vital, life-saving information.”[158] The relationship between the public and government officials should be a two-way street, where information flows both ways.

Department Budget Cuts

As department budgets shrink, agencies are forced to prioritize. The lack of funding is also another problem facing law enforcement and intelligence agencies. A social media monitoring application or program does not need to be costly. The specific features that the FBI requested for its own social media tool are for the most part already available online through free and low cost services. A high percentage of what it is seeking can even be found on a free Google Dashboard.

First, the FBI’s request for “instant notifications of breaking events, incidents, and emerging threats” and the ability to monitor keywords and strings in all publicly available media could be fulfilled through free social media monitoring platforms such as Social Mention, which tracks trending topics, the frequency of topics, and the general sentiment of a

[156] Ibid.

[157] Fresenko, “Social Media Integration into State-operated Fusion Centers…,” p. 51.

[158] Ibid, p. 52.

topic.[159] The site allows a user to search all major SNS (Twitter, Facebook, Tumblr, etc.) for keywords in tweets, public status updates, and open discussions online.

Second, the request for access to geospatial maps that could plot data such as "U.S. Domestic terrorist data," weather conditions, and video feeds from traffic cameras could be for the most part, discovered through a Google search, Google Maps, and Google Earth. Even open source sites provide live maps of air traffic, weather conditions, and live traffic feed on highways and busy streets.[160] Free sites such as FlightAware allow users to search for the course and progress of any flight. The user can also search by airport, flight number, operator, or aircraft type. Open source websites also provide live weather radars displaying weather patterns around the world and country. These sites include livewxradar.com, weather.com, and the National Weather Service's Doppler radar services.

In relation to live video of traffic, websites such as Trafficland work with state departments of transportation (DOT) and provide over 10,000 live traffic cameras across the country. Most of the live feed is accessed for free and is searchable by state, region, and city; however, the service also offers dashboards that allow the user to create a virtual control room for a fee. The service also permits the user to view the traffic footage from a smart phone using its phone application. Although not all states are currently synced with Trafficland's system, it is continuing to grow. This demonstrates how this type of technology is already available and how it can be affordably adopted into FBI's monitoring application. These types of open source services were utilized during the Exercise 24 Mexico (X24) event to display live air traffic, and weather radars in order to gain situational awareness. Furthermore, the exercise also demonstrated how these low-cost technologies could be adapted to different types of crises and situations.

Also, Google Translate could satisfy the need for an immediate translation of tweets and other publicly available posts into English, which was also utilized during X24, since the exercise involved both American and Mexican government participants. Another FBI request could be partially fulfilled through Flickr's search options. The FBI has asked for an application, which would allow a user to quickly narrow a search to a specific area or

[159] "Social Media Application"

[160] Ibid.

location. Flickr allows a user to easily search for pictures in a given region or city. Lastly, the request to "geospatially locate bad actors or groups and analyze their movements, vulnerabilities, limitations, and possible adverse actions" could be partially accommodated through the use of interactive Google Maps and Google Earth.[161]

Although, there are assuredly more free to low cost options available online, this was merely a demonstration of how these applications and tools are already available to agencies, which may be facing budget shortages. The general use of social media could actually save money considering it reduces the costs of traditional government-to-constituent communication and saves money and time on traditional investigative practices. For example, it is considerably less costly and simpler to support a Twitter page than employing mailers or working with the press, which isn't always apt to release a positive spin on the information provided to them. It is also considerably cheaper to perform an online social network search to discover a suspect's network of friends than to find and hire informants, who could provide similar information (although the latter method should not be entirely discarded considering it provides information that online searches cannot).

Other Issues Facing Government Entities

There are additional problems facing government entities from effectively adopting social media into either their communication with the public or investigations. These other problems should be further considered. These problems include 1) the rules and policies against the use of social media on government computers, and 2) the unfamiliarity with the functionality and nuances (including jargon and foreign languages) in social media by traditional law enforcement and intelligence community.

Since the popularity of personal activity on social network sites has risen in the last seven years, government agencies and departments have recognized the linked potential cyber security problems. As result, many agencies have blocked such sites as Facebook, MySpace, and Twitter on all government computers. In a survey, which included government employees, when asked about the top challenges of utilizing social networks, 41 percent of respondents pointed to governance and legal issues. In addition, 40 percent cited

[161] "Social Media Application"

alignment with agency mission as a challenge to adopting social media.[162] While the government is correct in protecting often classified computers from unsecured social networks, the regulations have created a mindset disinclined to utilizing social media in solving problems. Although agencies are wise to stress the security risks linked with social media, their missions and regulations should not hinder the appropriate use of it. Correct steps in information security (i.e. separate computers for classified information and internet and social media accessible computers, strong passwords, and employee training) should clam the security anxieties. With the correct protocols and leadership, government employees can feel less hindered and safer when using social media. Department heads and managers should also be well informed and teach their subordinates that the usage of SNS does fit within each agency's respective mission. This idea actually leads to another challenge for the effective implementation of social media: the unfamiliarity with the functionality and nuances in social media among the traditional law enforcement and intelligence communities.

If law enforcement or intelligence employees (i.e. agents, analysts, and managers) have only a basic understanding of social media and its nuances, this could hinder the big-picture application of it in investigations and intelligence gathering. While working for a federal law enforcement agency, the author witnessed the frustration and confusion when using social media in investigations. Some colleagues were intimidated with using technologies and jargon they did not understand, while others were uninterested and preferred traditional methods of investigation. With more and more adults using social media, generational ignorance should no longer be an excuse. If law enforcement is not where the criminals are, this can severely hurt the overall success of a division or even an entire agency. Even though most agencies provide training on social media, more should be done in the actual implementation. It would also be useful to hire more individuals with a firm understanding and knowledge of social media; moreover, individuals who are willing to continue to keep up with the ever-growing cyber world of social network technologies.

[162] Alice Lipowicz, "Agencies Question the Value of Social Media," *Federal Computer Week*, last modified December 20, 2011, http://fcw.com/articles/2011/12/20/government-agencies-going-more-social-but-still-worried-about-roi-survey-says.aspx.

Much of the jargon is difficult to initially understand, but with continued use and training, investigators and analysts will feel more at ease. With the lack of current literature on this particular issue, more could be researched on how social media tools can better be taught and implemented into the daily activities of law enforcement and intelligence agencies.

Overall, most government agencies have recognized the immense power of social media and its influence on society. Although the implementation of social media and monitoring tools has been successful in intelligence collection and investigations, it should not be the sole source of information. Social media should act as a supplement to more traditional methods. Together, government officials will find greater success.

CHAPTER 4

CONSTITUTIONAL AND LEGAL ISSUES FACING LAW IN UTILIZING SOCIAL MEDIA IN INVESTIGATIONS AND INTELLIGENCE GATHERING

The discussion of social media in intelligence collection and investigations would be incomplete without examining the legal and constitutional implications involved. In extracting information from newer technologies, there is much confusion as to which laws apply considering most laws have not kept pace with the rapidly evolving world of social media. Law enforcement and intelligence agencies do not exist in a free-for-all atmosphere where there are no regulations; however, most laws are ambiguous leaving government officials to guess or push the limits. Analogies to old laws and court decisions often are ineffective; this only reveals that laws should be clarified and updated.

This chapter will cover some of the constitutional issues, legal issues, and court cases affecting the U.S. government's social media exploitation. This is by no means an in depth conversation, but a basic discussion, which will hopefully open up to more questions and research. Suits of the government (DHS) by groups such as EPIC (Electronic Privacy Information Center) will likely blossom extensive legal opinions in this arena in the near future.[163]

Civil rights groups have consistently challenged the U.S. intelligence and law enforcement communities on its implementation of social media monitoring. The main constitutional issues revolving around social media are the Fourth Amendment (Freedom of Speech) and the First Amendment (protection against unlawful search and seizure).

[163] "EPIC Asks Congress to Suspend DHS Social Network Monitoring Program," Electronic Privacy Information Center, last modified February 15, 2012, http://epic.org/2012/02/epic-asks-congress-to-suspend-.html.

FOURTH AMENDMENT AND PRIVACY

The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issues, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searches and the persons or things to be seized.

Before 1967, the Supreme Court's interpretation was literal: the Fourth Amendment was not violated as long as there was no search of a person, or his tangible, material effects without a warrant. The 1928 court case *Olmstead v. United States* ruled that police wiretaps were not considered an illegal search under the Fourth Amendment since wiretaps did not violate "spatial privacy." Nevertheless, not all the justices agreed. The dissent written by Justice Brandeis argued that a literal reading of the Fourth Amendment "failed to recognize the changing societal conditions." As a result of the rulings; however, they "[reaffirmed] the physical trespass standard . . . [insulated] new police practices and investigative techniques from review by the courts."[164]

In the 1967 *Katz v. United States*, another wiretapping case, the Court reversed its previous ruling arguing, "The Fourth Amendment protects people, not places."[165] Justice Harlan's concurring opinion established a "twofold requirement, first, that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" In order to summon the protection of the Fourth Amendment, "both subjective and objective questions of reasonableness must be answered in the affirmative."[166]

In this case, law enforcement would have to obtain a warrant.[167] The *Katz* case set new precedence privacy. As the world has changed from landlines to cellular phones to

[164] Matthew J. Hodge, "The Fourth Amendment and Privacy Issues on the 'New' Internet: Facebook.com and MySpace.com," *Southern Illinois University Law Journal* 31 (2006): 95-122. http://heinonline.org/HOL/LandingPage?collection=journals&handle=hein.journals/siulj31&div=11&id=&page=

[165] Ibid., p. 100.

[166] Ibid.

[167] Ibid.

emailing to text messaging to social networking, the issue of privacy has lingered in public discourse.

"New technologies create interesting challenges to long established legal concepts . . . now personal computers, hooked up to large networks are so widely used that the scope of the Fourth Amendment core concepts of 'privacy' as applied to them must be reexamined."[168] The evolving nature of social media has put into question whether the Courts' ruling have any modern-day relevance. Associate Justice Clarence Thomas commented on the Court's pace in keeping up with technological changes. According to him, technological change within the Court was less important that that occurring on the outside:

> It's changed the way we work, but it's also changed some of the issues . . . I think you are al in for some interesting times because there used to be these zones of privacy . . . Things were over here in the private sphere and then the public sphere was over here. Now look how [they've] merged. You put something on your Facebook, [and] it's there on somebody's hard drive forever . . . We also see it with respect to how the government can obtain information in the criminal justice context. {The government doesn't actually have to come onto property now, to look into your private affairs . . . I think you all are in for the brave new world of technology in a way that we, of course, couldn't have anticipated."[169]

Social media sites are definitely a part of this "brave new world" Justice Thomas describes. In an online community where users openly share personal information, which would not have been shared even five years ago, social media has attracted the attention of both welcomed and unwelcomed eyes. Everyone from criminals to law enforcement can be considered unwelcomed. The usage of social media as an investigative tool has disturbed many critics. For the most part, civil liberties advocates argue that law enforcement violates assumed Fourth Amendment rights when it uses information gathered from sites such as Facebook or Twitter.[170]

Are these advocates justified in their argument? SNS are "built upon a bedrock of voluntary disclosure. The user shares their names, pictures, location, etc. and this "information is communicated to, and stored upon, the social networking web site's servers .

[168] Petrashek, "The Fourth Amendment and the Brave New World…"

[169] Ibid.

[170] Ibid.

. .” Voluntary disclosure of information to third parties and the role it plays in personal privacy is called the “third-party doctrine.”[171]

United States v. Miller laid precedent on the level of protection an individual has against government searches of personal information held by a third parties. Banks were considered the third party in this case. The Supreme Court ruled that the bank was not required to inform its customers if it turned over financial records to the government. In this case, it was the ATF. As such, the customer could not invoke Fourth Amendment rights against illegal search and seizure because the bank records were bank property, in which the customer had no legitimate “expectation of privacy.” This produces the question of whether this third party doctrine actually does apply to social network sites.[172]

One recent case involving Twitter, national security issues, and privacy occurred when federal officials demanded that Twitter hand over data from three different accounts connected to Julian Assange, the Wikileaks founder. Wikileaks, a watchdog website, posted thousands of sensitive government documents on its site. Instead of handing over the requested information, Twitter sued the government to lift a gag order that prevented the company from informing their account holders that the government had requested their data. Although Twitter lost the case, it “beta-tested a spine” by challenging the status quo, where social media sites typically comply with government requests.[173] In this case, the third party doctrine did apply to Twitter.

Both the existing DHS program and the FBI’s potential social media application have captured the attention of advocacy groups. In defense, an FBI spokesman stated that the proposed application would only collect information on publicly available information and would not be used to “focus on specific individuals or groups.”[174] The Electronic Privacy Information Center (EPIC) has remained skeptical commenting that the program should not

[171] Petrashek, “The Fourth Amendment and the Brave New World…”

[172] Matthew J. Hodge, “The Fourth Amendment and Privacy Issues on the ‘New’ Internet…”

[173] Mashable, “5 Ways Twitter is Changing Media Law,” accessed March 1, 2012, http://mashable.com/2012/01/30/how-twitter-changes-media-law/.

[174] “FBI Seeks Social Media Monitoring Tool,” *Computer World*, accessed February 16, 2012, http://www.computerworld.com/s/article/9224235/FBI_seeks_social_media_monitoring_tool.

proceed without proper oversight.[175] In a Congressional Hearing about its monitoring program, DHS officials also defended their program. They argued that it was not intended to target individuals or groups, but to gain situational awareness. Critics have argued that DHS's testimonies on its program were inconsistent with how the department actually utilizes the program and that its activities violate privacy.[176]

These two programs have brought further discussion on the controversy of whether searching supposedly publicly available information derived from social media is legal and protects users' privacy. According to the two-prong approach set by the *Katz v. United States* case, the monitoring of publicly available social media without a warrant may or may not violate Fourth Amendment rights. According to the *Katz* ruling, the person must have exhibited an expectation of privacy. The controversy arises when social media users do not fully understand their privacy settings on their respective sites. If the user believes its settings are private, but they are indeed public, this creates confusion and does not clearly answer whether the person had an expectation of privacy.

The second prong asks whether society deems the expectation as reasonable. Society's opinions on whether law enforcement or intelligence agencies can mine through public data made available through social media vary. However, for the most part, the courts have rejected any notions that information on social network sites should be considered private.

Although privacy on social media sites remains murky, the courts have provided some precedence. The courts have actually rejected the privacy of SNS in realm of discovery for three reasons. The courts are unwilling to grant privacy protection "to information deliberately placed in the public sphere."[177] The user has willingly provided that information. Second, the courts favor production of information over privacy in SNS accounts because the information drawn from SNS is "reasonably calculated to lead to the

[175] "FBI Seeks Social Media…"

[176] "EPIC vs. Department of Homeland Security: Media Monitoring," *Electronic Privacy Information Center*, accessed March 17, 2012, http://epic.org/foia/epic-v-dhs-media-monitoring/.

[177] Andrew C. Payne, "Twitigation: Old Rules in a New World," *Washburn Law Journal* 49, no. 3 (2010): 841-870, http://washburnlaw.edu/wlj/49-3/articles/payne-andrew.pdf.

discovery of admissible evidence as is relevant to the issues in [the] case."[178] Third, the courts have held that social media users have no expectation of privacy when they knowingly post information on very popular websites. These three reasons were in context of a court setting. Would these court opinions also apply to intelligence agencies?

In his article, "Twitigation: Old Rules in a New World," Andrew C. Payne argued that these earlier interpretations of social media by the courts may be early indications of how the courts will act in the future. He argues that the current path should change because social networking information is unique from other forms of information. The *Katz* approach and other approaches often do not neatly define these issues.[179] Because old forms of information discovery are used as analogies, the courts have ignored the implications brought on by newer technologies.

Nevertheless, government entities continue to sift through publicly available information because it abides by the "plain view" doctrine that something can be searched if in plain view in both the physical and electronic sense. Under this notion, if the information is available publicly, it is considered in "plain view" and law enforcement is not conducting an "illegal search."[180] This doctrine permits law enforcement to access public profiles and any social media postings not secured with privacy settings.

The NSA's monitoring programs have also come under scrutiny. To understand the argument, it is important to understand the origins of the agency. In 1952, President Harry Truman through an executive order created the National Security Agency's (NSA). The order restricted NSA's spying on foreign governments. In 1978, Foreign Intelligence Surveillance Act (FISA) legislation banned the NSA from domestic eavesdropping without a warrant. Early activities included intercepting telephone and telegraphic communications. As the world became more digital, the NSA began a heavier monitoring program of telephone and Internet activity. The wireless world of cellular phones and Internet access blurred the lines; critics began arguing that the NSA was beginning to monitor American

[178] Payne, "Twitigation: Old Rules…"

[179] Ibid.

[180] Martha S. Stonebrook and Richard A. Stubbs, "Social Networking in Law Enforcement – Legal Issues," Americans for Effective Law Enforcement, accessed January 4, 2012, http://www.aele.org/los2010_sm-visual.pdf.

citizens, which was beyond its scope of power. The collection and analysis of the data from "little-known sources . . . blur the lines between domestic and foreign intelligence gathering."[181]

In response to the 9/11 attacks, NSA officials justified their expanded powers based on the 1981 Executive Order 12333, which was intended to expand the powers and responsibilities of the intelligence community.[182] Soon after the attacks, a classified executive order "opened the door for the NSA to incorporate more domestic data in its searches."[183] These executive orders have become the basis of the NSA's expanded intelligence role.

Moreover, critics argued the NSA is violating Fourth Amendment rights with its data-mining program that allegedly sifts not only through cellular phone calls, financial transactions, emails, but potentially social media activity of American citizens. Nevertheless, the NSA has based its data-sifting program's legality on the 1979 court case *Smith v. Maryland*, which decision permitted the records of phone calls, but not the actual conversations, to be collected sans warrant.[184]

FIRST AMENDMENT AND FREE SPEECH

Others have argued that law enforcement monitoring of social media also affects First Amendment rights. For example, Representative Patrick Meehan of Pennsylvania stated that DHS's social media has a "chilling effect" on not only privacy rights, but also "people's freedom of speech and dissent against their government." As mentioned in Chapter 3, DHS has used a system that collects and analyzes information from SNS about terrorist threats and natural disasters. However, critics like EPIC believe that "Law-enforcement agency monitoring of online criticism and dissent chills legitimate criticisms of the government, and

[181] Siobhan Gorman, "NSA's Domestic Spying Grows…"

[182] Exec. Order 12333 of Dec. 4, 1981, 46 Fed. Reg. 59941, 3 C.F.R., 1981 Comp., p. 200.

[183] Ibid.

[184] Ibid.

implicates the First Amendment." Moreover, government programs such as this send the "chilling message" that SNS users are "being watched."[185]

DHS Secretary Janet Napolitano and other DHS officials defended the program arguing that the monitoring system is concerned with the "what" and not the "who" as far as collecting data from SNS. Furthermore, the department does not follow specific individuals, but instead searches for specific key words and websites. Secretary Napolitano stated in response to the British travelers, who were held in custody and questioned after the tweeting incident, that it was a result of a tip and not a monitoring of Twitter. "We aren't sitting there monitoring social media looking for stuff. That's not what we do," she stated.[186]

Instead, critics of the program believe the government is using the collected data for ulterior motives such as monitoring individuals who post negative comments about DHS policies. Ginger McCall, director of EPIC, in a letter to Congress, wrote, "The search terms that DHS has chosen to monitor sweep in vast amounts of First Amendment protected speech that is entirely unrelated to [DHS's] mission."[187] The issue was further pronounced when the two British travelers were arrested for their Twitter comments.

Whether they are correct or not, the Supreme Court has not yet taken on any case involving the First Amendment and social media in an intelligence gathering situation. Most free speech cases involved social media in school or work settings. For instance, the Court rejected in January of 2012, a case involving a student who defamed a school official on a SNS and the following punishment form the school board. Although the case deals more with student-speech issue, the case could have set more specific precedence for expression on SNS. Instead, rulings hark back to the 1969 Supreme Court precedent set by *Tinker v. Des Moines Independent Community School District* which ruled that student expression could not be suppressed unless school officials conclude it would "materially and substantially disrupt the work and discipline of the school." Some lower courts argued that this

[185] Josh Smith, "House Panel Decries 'Chilling' Effect of DHS Social-Media Monitoring," Technology, *National Journal*, last modified February 16, 2012, lhttp://www.nationaljournal.com/tech/house-panel-decries-chilling-effect-of-dhs-social-media-monitoring-20120216.

[186] Ibid.

[187] Alex Rash, "Social Media Brings New Age Challenges to Freedom of Speech," *NWMissourian,* last modified March 29, 2012, http://www.nwmissourinews.com/news/article_abf65c3e-6e30-11e1-8941-0019bb30f31a.html.

application is “out of touch with today’s reality.”[188] Cases similar to *Tinker* reveal the unsatisfactory results stemming from old and no longer relevant rulings.

Twitter managed to embroil itself with another issue involving civil liberties. Shurat HaDin, the Israel Law Center, threatened to sue Twitter unless it shut down the accounts run by terrorist groups such as Hezbollah and al-Shabab. The center stated, “Twitter’s complicit service to known foreign terrorist organizations is not only morally irresponsible, it is also illegal.”[189] The group’s threat was based on the *Holder v. Humanitarian Law Project*, which upheld a “controversial portion of the Patriot Act” which banned support to terrorists. Besides traditional support such as money or arms, it prohibited anyone from offering “any . . . service, . . . training, [or] expert advice or assistance.”[190]

Twitter refused to comply with the request. Not only basing its decision on the grounds of free speech, the company believed shutting down the terrorists’ accounts could not silence terrorist groups. Twitter argued that if an account is shut down, terrorists will simply open a new account or move to another social media platform. Commenting on the requests, a Twitter spokesman tweeted, “How many accounts would #US government be able to close before realizing the futility in their attempt?”[191] Critics also argued that the Patriot Act language upheld by *Holder*, which prohibited forms of support to terrorists “encroached on free speech rights and criminalized dialogue with terrorists.”[192] The degradation of free speech continues to concern civil liberties advocates.

There have been other efforts through the years, which have led critics to believe the government is attempting to censor speech online. The 1996 Communication Decency Act (CDA) was the first legislative piece to regulate the then relatively new Internet. It sought to

[188] David Kravets, “Supreme Court Rejects Student Social Media Cases.” Threat Level, *Wired*, last modified January 17, 2012, http://www.wired.com/threatlevel/2012/01/scotus-student-social-media/.

[189] Christopher Williams, “Twitter Threatened with Court Over Hezbollah Tweets,” *The Telegraph*, December 30, 2011, http://www.telegraph.co.uk/technology/twitter/8984705/Twitter-threatened-with-court-over-Hezbollah-tweets.html

[190] Adam Rawnsley, “Twitterfight! Group Threatens Lawsuit Over Terror Tweets,” Danger Room, *Wired*, last modified January 2, 2012, http://www.wired.com/dangerroom/2012/01/twitterfight-group-threatens-lawsuit-over-terror-tweets/.

[191] Ibid.

[192] Ibid.

regulate pornography and material that was considered "obscene or indecent." Nevertheless, after protests and challenges from civil liberties groups, who argued it would inevitably limit other forms of speech, federal judges struck down the portions of the CDA that appeared to have limited free speech.[193, 194, 195]

More recently, the Stop Online Piracy Act/ Protect IP Act (SOPA/PIPA) anti-piracy bills were drafted to prevent copyright infringement and intellectual property theft; however, sites such as Wikipedia, Reddit, and WordPress argued that it would infringe upon expression on the Internet and all protested by blacking out their sites. The bills would empower the Justice Department to go after foreign websites committing intellectual property theft and "force U.S.-based companies like Internet service providers . . . to cut off ties with those sites."[196] The CDA and the recent SOPA/PIPA bills all created so much controversy that they ultimately failed. History illustrates the unpopularity of censoring speech online.

There have been other incidents when Congress has attempted to regulate speech online. In 2008, Senator Joseph Lieberman demanded YouTube take down videos uploaded by Islamic terrorists. After Lieberman sent a letter to Google, the company removed over eighty videos from YouTube. The senator remained unsatisfied that hundreds more remained on the website. YouTube responded that the videos it did take down featured "gratuitous violence, advocated violence, or used hate speech." The videos that remained did not include any of those offenses and thus did not violate the site's guidelines. YouTube did not agree to take down every video from terrorist groups unless the videos violated its guidelines. YouTube's blog stated, "While we respect and understand his views, YouTube

[193] Rash, "Social Media brings new age challenges…"

[194] Timothy E. Nichols, "The Communications Decency Act: A Legislative History," *PDF Cast*, last modified February 19, 2011, http://pdfcast.org/pdf/the-communications-decency-act-a-legislative-history.

[195] "Communications Decency Act," *Wikipedia*, last modified April 17, 2012, http://en.wikipedia.org/wiki/Communications_Decency_Act.

[196] Stephanie Condon, "SOPA, PIPA: What You Need to Know," Political Hotsheet, *CBS News*, January 18, 2012, http://www.cbsnews.com/8301-503544_162-57360665-503544/sopa-pipa-what-you-need-to-know/.

encourages free speech and defends everyone's right to express unpopular points of view."[197] YouTube's refusal to remove all requested material is another demonstration of the social media community's desire to protect First Amendment rights.

Until the courts rules on a case dealing with these social media issues, many questions will still remain on what can be said and what kind of information can exist online. In addition, Congress will have to assist in the process of updating the current laws to cater to new technologies. However, new laws should not be overly burdensome that investigations and national security are negatively affected. There must be a delicate balance. In the meantime, law enforcement and intelligence agencies must use common sense in its utilization of social media.

[197] Jack Date. "Lieberman: YouTube Not Doing Enough to Remove Terrorist Content," *ABC News*, May 19, 2008, http://abcnews.go.com/TheLaw/LawPolitics/story?id=4889745&page=2.

CHAPTER 5

CONCLUSION

Evolving communication technologies like social media have already transformed society in the short span of its life thus far. We know that clandestine groups like Islamic terrorist groups and drug cartels are exploiting these sites for their own purposes. In order to protect the nation, law enforcement and intelligence agencies must continue to utilize social media as a tool in investigations and intelligence gathering. Social media is an important supplement to all traditional government activities and though it is effective, it should never be the only source of intelligence. Although it can produce effective intelligence, it has its shortcomings: the tone of a status update or tweet cannot be certain, there exists massive amounts of unrelated data which is swiped up, and social media cannot always provide accurate context to certain information.

Social media monitoring tools do not need to be expensive in order to be effective. Moreover, increased efforts to streamline these tools will render them more effective for intelligence sharing and communication. Although, law enforcement and intelligence agencies should utilize social media in their respective missions, they must heed to the law and ensure the protection of constitutional rights. Regardless of out of date laws, intelligence communities and law enforcement should not wait to be challenged. This will only fuel the public's mistrust and destroy the organizations' credibility. Using social media as a tool should be balanced; it should not be hindered by over-aggressive privacy laws, nor should it encroach on civil liberties. The balance is delicate, but can be achieved with thoughtful expertise.

Although this research covered several issues facing social media in law enforcement and national security issues, it also opens up more questions and provides ideas for those who may be more technically knowledgeable. The hope of this study is that through this research, more effort will be placed in creating low-cost social media platforms that will benefit both citizen and government. It is also the hope of this study that more research will add to the legal understandings and implications of social media in a free society and in the larger world where different nations have very different laws and expectations of privacy for their citizens.

REFERENCES

Albanesius, Chloe. “Terrorists in Second Life? Hogwash says CEO.” *PC Magazine,* April 1, 2008. http://www.pcmag.com/article2/0,2817,2280660,00.asp.

Albrechtslund, Anders. “Online Social Networking as Participatory Surveillance.” First Monday. Last modified March 3, 2008. http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2142/1949.

Alexa. “Alexa Top 500 Global Sites.” Accessed February 2, 2012. http://www.alexa.com/topsites.

Angulo, Erika, and Wilma Hernandez. “Mexican Journalist on Drug Lords: If They’re Going to Kill You, They’re Going to Kill You.” World Blog. *NBC News,* February 24, 2012. http://worldblog.msnbc.msn.com/_news/2012/02/24/10497924-mexican-journalist-on-drug-lords-if-theyre-going-to-kill-you-theyre-going-to-kill-you.

AnonTwttr. “Tweet Anonymously.” Accessed March 9, 2012. http://anontwttr.fox21.at/.

Bernard, Doug. “Does Social Media Help or Hurt Terrorism?” *Voice of America.* Last modified January 21, 2012. http://blogs.voanews.com/digital-frontiers/2012/01/21/does-social-media-help-or-hurt-terrorism/.

Bowley, Graham and Matthew Rosenberg. “U.S. Deplores Video of Marines Urinating on Taliban.” *The New York Times*, January 12, 2012. http://www.nytimes.com/2012/01/13/world/asia/video-said-to-show-marines-urinating-on-taliban-corpses.html?pagewanted=all.

Boyd, Danah M. and Nicole B. Ellison. “Social Network Sites: Definition, History, and Scholarship.” *Journal of Computer-Mediated Communication* 13 (2007): 210–230. doi:10.1111/j.1083-6101.2007.00393.x.

Burnett, John. “Mexican Drug Cartels Now Menace Social Media.” *NPR,* September 23, 2011. http://www.npr.org/2011/09/23/140745739/mexican-drug-cartels-now-menace-social-media.

Callaghan, Heather. “British Tourists Arrested for Tweets of Terror.” *Activist Post*. Last modified January 31, 2012. http://www.activistpost.com/2012/01/british-tourists-arrested-for-tweets-of.html.

Castillo, Mariano. "Bodies Hanging from Bridge in Mexico are Warning for Social Media Users." World. *CNN*, September 14, 2011. http://articles.cnn.com/2011-09-14/world/mexico.violence_1_zetas-cartel-social-media-users-nuevo-laredo?_s=PM:WORLD.

Cattan, Nacha. "Mexico's Drug War Hits YouTube Against Rival Groups." *Christian Science Monitor,* November 5, 2010. http://www.csmonitor.com/World/Americas/2010/1105/How-Mexican-drug-gangs-use-YouTube-against-rival-groups.

CBS News. "FBI: Ex-Soldier Tried to Aid Terrorists." *CBS News*, January 9, 2012. http://www.cbsnews.com/8301-201_162-57355319/fbi-ex-soldier-tried-to-aid-terrorists/.

Cisco. "Mexican Crime Groups Expand into Cyber World." Cyber Risk Report. Accessed September 22, 2011. http://www.cisco.com/web/about/security/intelligence/CRR_jun13-19.html.

Collins World English Dictionary Online. "Definition of medium." Accessed January 2, 2012. http://www.collinsdictionary.com/dictionary/english/medium.

Computer World. "FBI Seeks Social Media Monitoring Tool." Accessed February 16, 2012. http://www.computerworld.com/s/article/9224235/FBI_seeks_social_media_monitoring_tool.

Condon, Stephanie. "SOPA, PIPA: What You Need to Know" Political Hotsheet. *CBS News,* January 18, 2012. http://www.cbsnews.com/8301-503544_162-57360665-503544/sopa-pipa-what-you-need-to-know/.

Date, Jack. "Lieberman: YouTube Not Doing Enough to Remove Terrorist Content." *ABC News,* May 19, 2008. http://abcnews.go.com/TheLaw/LawPolitics/story?id=4889745&page=2.

Daw, David. "Criminals find new uses for 3D printing." *PC World.* Last modified October 10, 2011. http://www.pcworld.com/article/241605/criminals_find_new_uses_for_3d_printing.html.

Denning, Dorothy E. "A View of Cyberterrorism Five Years Later." Center on Terrorism and Irregular Warfare. *Naval Postgraduate School.* Accessed January 3, 2012. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA484928&Location=U2&doc=GetTRDoc.pdf.

Dickinson, Boonsri. "Infographic: 80% of Robbers Check Twitter, Facebook, Google Street View." *Smart Planet*. Last modified November 1, 2011. http://www.smartplanet.com/blog/science-scope/infographic-80-of-robbers-check-twitter-facebook-google-street-view/11082.

Drapeau, Mark and Linton Wells II. "Social Software and National Security: An Initial Assessment." Center for Technology and National Security Policy. *National Defense University*. Accessed September 23, 2011. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA497525.

Drug Enforcement Administration. "Case Number: 10-0166-F." Accessed February 22, 2012. https://www.eff.org/sites/default/files/filenode/social_network/20100514_dea_socialnetworking.pdf

Drug Enforcement Administration. “Social Media for Intelligence Professionals.” (Handout from DNI Open Source Center, San Diego, CA, January 25, 2012.)

Electronic Privacy Information Center. “EPIC vs. Department of Homeland Security: Media Monitoring.” Accessed March 17, 2012. http://epic.org/foia/epic-v-dhs-media-monitoring/.

———. “EPIC Asks Congress to Suspend DHS Social Network Monitoring Program.” Last modified February 15, 2012. http://epic.org/2012/02/epic-asks-congress-to-suspend-.html.

Exec. Order 12333 of Dec. 4, 1981, 46 Fed. Reg. 59941, 3 C.F.R., 1981 Comp., p. 200.

Federal Bureau of Investigation’s Facebook page. Accessed March 10, 2012. www.facebook.com/fbi.

Federal Business Opportunities. “Social Media Application.” *FedBizOpps.* Last modified February 14, 2012. https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=c6577735633 4dab8685984fa74bfd636&_cview=1.

Flip the Media. “Blogging and Social Networking Turn Deadly in Mexico.” Last modified December 23, 2011. http://flipthemedia.com/2011/12/why-blogging-and-social-networking-in-mexico-can-turn-deadly/.

Fox News. “Terrorists Targeting Children via Facebook, Twitter.” *Fox News,* March 15, 2010. http://www.foxnews.com/scitech/2010/03/15/terrorists-targeting-children-via-facebook-twitter/.

Fresenko, Victoria L. “Social Media Integration into State-operated Fusion Centers and Local Law Enforcement: Potential Uses and Challenges.” *Naval Postgraduate School.* Accessed February 22, 2012. http://www.hsdl.org/?view&did=11536.

Gorman, Siobhan. “NSA’s Domestic Spying Grows as Agency Sweeps Up Data.” *The Wall Street Journal,* March 10, 2008. http://online.wsj.com/article/SB120511973377523845.html.

Graham, Ronan. “Are Mexico Drug Gangs Drafting Hackers?” *Borderland.* Last modified July 18, 2011. http://www.borderlandbeat.com/2011/07/are-mexico-drug-gangs-drafting-hackers.html.

Håland, Leon. “Time to Reach 10 Million Users.” *Google+*. Last modified September 30, 2011. https://plus.google.com/112418301618963883780/posts/D2Rz5rdciWE.

Hanson, Wayne. “How Social Media is Changing Law Enforcement.” Justice and Public Saftey. *GovTech.* Last modified December 2, 2011. http://www.govtech.com/public-safety/How-Social-Media-Is-Changing-Law-Enforcement.html.

Hide My Ass. “Hide My Ass! Free Proxy and Privacy Tools – Surf the Web Anonymously.” Accessed January 31, 2012. http://hidemyass.com/.

Hodge, Matthew J. “The Fourth Amendment and Privacy Issues on the ‘New’ Internet: Facebook.com and MySpace.com.” *Southern Illinois University Law Journal* 31 (2006): 95-122. http://heinonline.org/HOL/LandingPage?collection=journals&handle=hein.journals/siulj31&div=11&id=&page=.

IIP State. “IIP CO.NX. Online Destination for Global Digital Diplomacy.” Accessed February 7, 2012. http://conx.state.gov/.

Ingram, Matthew. “Twitter Users Beware: Homeland Security Isn’t Laughing.” *Bloomberg Businessweek.* Last modified January 30, 2012. http://www.businessweek.com/technology/twitter-users-beware-homeland-security-isnt-laughing-01302012.html

International Business Times. “Norway Killings: Shooter Used Video Games as Training Methods.” Last modified July 27, 2011. http://au.ibtimes.com/articles/187509/20110727/anders-behring-brejvik-activision-modern-warfare-world-of-warcraft-norway-killings.htm.

Jacobson, Michael. “Terrorist Financing and the Internet.” *Studies in Conflict & Terrorism* 33, no. 4 (2010): 353-363.

Jagatic, Tom, Nathaniel Johnson, Markus Jakobsson, and Filippo Menczer. “Social Phishing.” School of Informatics. *Indiana University, Bloomington*. Last modified December 12, 2005. http://www.indiana.edu/~phishing/social-network-experiment/phishing-preprint.pdf.

Johnson, Carrie. “JihadJane, an American Woman, Faces Terrorism Charges.” *The Washington Post*, March 10, 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/03/09/AR2010030902670.html.

Kahn, Jeremy. “Mumbai Attackers Use Sophisticated Technology.” *The New York Times*, December 9, 2008. http://www.nytimes.com/2008/12/09/world/asia/09iht-attack.1.18517890.html.

Katz, Rita, and Michael Kern. “Terrorist 007, Exposed.” *The Washington Post,* March 26, 2006. http://www.washingtonpost.com/wp-dyn/content/article/2006/03/25/AR2006032500020.html.

Kessler, Ronald. “Facebook, YouTube, and Terrorists—A Deadly Mix.” *Newsmax*. Last modified February 18, 2011. http://www.newsmax.com/RonaldKessler/Facebook-YouTube-FBI-Terrorists/2011/02/18/id/386589.

Kohlman, Evan F. “The Anti-Social Network: Countering the Use of Online Social Networking Technologies by Foreign Terrorist Organizations.” Accessed January 21, 2012. http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20Kohlmann%5B1%5D.pdf.

Kravets, David. “Supreme Court rejects student social media cases.” Threat Level. *Wired.* Last modified January 17, 2012. http://www.wired.com/threatlevel/2012/01/scotus-student-social-media/.

Lehrman, Yosef. “The Weakest Link: The Risks Associated with Social Networking Websites.” *Journal of Strategic Security 3*, no. 2 (2010): 63-72. http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1014&context=jss.

Lipowicz, Alice. “Agencies Question the Value of Social Media.” *Federal Computer Week.* Last modified December 20, 2011. http://fcw.com/articles/2011/12/20/government-agencies-going-more-social-but-still-worried-about-roi-survey-says.aspx.

Lococitato. “Loco citato. Mapping Social Networks.” Accessed February 2, 2012. http://www.lococitato.com/.

Lyon, Ethan. “Emergence of Online Social Gaming.” *Sparxoo*. Last modified August 2, 2010. http://sparxoo.com/2010/08/02/nielsen-study-social-gaming/.

Manuel-Logan, Ruth. “Facebook Warrants by Law Enforcement Agencies Surge.” *All Facebook.* Last modified July 13, 2011. http://www.allfacebook.com/facebook-warrants-by-law-enforcement-agencies-surge-2011-07.

Mashable. “5 Ways Twitter is Changing Media Law.” Accessed March 1, 2012. http://mashable.com/2012/01/30/how-twitter-changes-media-law/.

McCants, William. “Subcommittee Hearing: ‘Jihadist Use of Social Media – How to Prevent Terrorism and Preserve Innovation.’ Testimony of William McCants.” Committee on Homeland Security’s Subcommittee on Countertorrism and Intelligence. Accessed January 14, 2012. http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20McCants.pdf.

Mello, John P. Jr. “FBI Looking to ‘Friend’ Terrorists.” Cybersecurity. *Tech News World.* Last modified January 30, 2012. http://www.technewsworld.com/rsstory/74295.html.

Miller, Carolyn and Dawn Shepherd. “Blogging as a Social Action: A Genre Analysis of the Weblog.” *Into the Blogosphere: Rhetoric, Community, and Culture of Weblogs*. Last modified November 30, 2004. http://blog.lib.umn.edu/blogosphere/blogging_as_social_action_a_genre_analysis_of_the_weblog.html.

Moore, Emily. “Killed for Tweeting - Mexican Cartel Drug Hangs Couple From bridge as Warning After Torture.” *Wish I Didn’t Know*. Last modified September 16, 2011. http://wishididntknowthat.tumblr.com/post/10290242074/killed-for-tweeting-mexican-cartel-drug-hangs.

National Gang Intelligence Center. “2011 National Gang Threat Assessment.” Accessed February 2, 2012. http://www.fbi.gov/stats-services/publications/2011-national-gang-threat-assessment/2011-national-gang-threat-assessment-emerging-trends.

National Public Radio. “How does the CIA use Social Media?” *NPR.* Last modified November 7, 2011. http://www.npr.org/2011/11/07/142111403/how-does-the-cia-use-social-media.

Nesbitt, Scott. “What is Microblogging?” Tech Tips. *Geeks.com*. Last modified April 26, 2009. http://www.geeks.com/techtips/2009/what-is-microblogging.htm.

Nichols, Timothy E. “The Communications Decency Act: A Legislative History.” *PDF Cast*. Last modified February 19, 2011. http://pdfcast.org/pdf/the-communications-decency-act-a-legislative-history.

Northcutt, Stephen. “Spear Phishing.” Security Laboratory. *SANS Institute*. Last modified May 9, 2007. http://www.sans.edu/research/security-laboratory/article/spear-phish.

NR Staff. “’Blogger’s Beware’- Drug Cartel Mutilate Two Blogger’s In Mexico!” *Naija Resource*. Last modified September 16, 2011. http://www.naijapidginenglish.com/2011/09/16/bloggers-beware-drug-cartel-mutilate-two-bloggers-in-mexico/.

NTD Television. “Terrorism at Work in Social Networks.” Accessed February 13, 2012. http://english.ntdtv.com/ntdtv_en/news_middleeast_africa/2012-01-24/terrorism-at-work-in-social-networks.html.

Okeowo, Alexis. “To Battle Cartels, Mexico weighs Twitter Crackdown.” *Time,* April 14, 2010. http://www.time.com/time/world/article/0,8599,1981607,00.html.

Osman, Hoda. “Alleged Terrorists Used Social Network Sites” *CBS News*, May 19, 2010. http://www.cbsnews.com/8301-31727_162-20005405-10391695.html.

Pan, Joann. “FBI Uses Social Media to Catch Murder Suspect Who Stole $2.3 Million [VIDEO].” Social Media. *Mashable.* Last modified March 9, 2012. http://mashable.com/2012/03/09/kenneth-konias-wanted-fugitive/.

Payne, Andrew C. “Twitigation: Old Rules in a New World.” *Washburn Law Journal* 49, no. 3 (2010): 841-870. http://washburnlaw.edu/wlj/49-3/articles/payne-andrew.pdf.

Petrashek, Nathan. "The Fourth Amendment and the Brave New World of Online Social Networking." *Marquette Law Review* 93, no. 4 (2010): 1-36, http://scholarship.law.marquette.edu/cgi/viewcontent.cgi?article=5029&context=mulr.

Pew Internet. “Who uses what social networking site platform.” *Pew Internet & American Life Project*. Accessed February 2, 2012. http://www.pewinternet.org/Reports/2011/Technology-and-social-networks/Part-2/Platform.aspx.

ProtectMyID. “FBI Friday: Be Prudent When Posting Images Online.” *ProtectMyID* (blog), April 13, 2012. http://blog.protectmyid.com/2012/04/13/fbi-friday-be-prudent-when-posting-images-online/.

Public Intelligence. “Video: DHS Testimony on Social Networking and Media Monitoring.” *Global Research*. Last modified February 18, 2012. http://globalresearch.ca/index.php?context=va&aid=29369.

Randol, Mark A., “Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches.” *Congressional Research Service.* Last modified January 14, 2009. http://www.fas.org/sgp/crs/intel/RL33616.pdf.

Rash, Alex. “Social Media Brings New Age Challenges to Freedom of Speech.” *NWMissourian*. Last modified March 29, 2012.

http://www.nwmissourinews.com/news/article_abf65c3e-6e30-11e1-8941-0019bb30f31a.html.

Rawnsley, Adam. “Twitterfight! Group Threatens Lawsuit Over Terror Tweets.” Danger Room. *Wired.* Last modified January 2, 2012. http://www.wired.com/dangerroom/2012/01/twitterfight-group-threatens-lawsuit-over-terror-tweets/.

Reuters. “Mexican Social media boom draws drug cartel attacks.” Last modified September 27, 2011. http://www.reuters.com/article/2011/09/27/us-mexico-drugs-idUSTRE78Q6H220110927.

Rollins, John. “Terrorist Use of the Internet: Information Operation in Cyberspace.” CRS Report for Congress. Accessed October 2, 2011. http://www.fas.org/sgp/crs/terror/R41674.pdf.

———. “Fusion Centers: Issues and Options for Congress,” CRS Report for Congress. Last modified January 18, 2008. http://www.fas.org/sgp/crs/intel/RL34070.pdf.

Rollins, John, and Clay Wilson. “Terrorist Capabilities for Cyberattack: Overview and Policy Issues.” CRS Report for Congress. Last modified January 22, 2007. http://www.fas.org/sgp/crs/terror/RL33123.pdf.

Sawers, Paul. “Google+ Reached 10m Users in 16 Days. Want to Know How Long it Took Facebook and Twitter?” *The Next Web*. Last modified July 22, 2011. http://thenextweb.com/google/2011/07/22/google-reached-10m-users-in-16-days-want-to-know-how-long-it-took-facebook-and-twitter/.

Scotsman. “Terrorists recruiting on net via Facebook.” Last modified February 16, 2008. http://www.scotsman.com/news/terrorists_recruiting_on_net_via_facebook_1_1429940.

SecretTweet. “SecretTweet (secrettweet) on Twitter.” Accessed January 31, 2012. http://twitter.com/secrettweet/.

Shachtman, Noah. “Exclusive: Google, CIA Invest in ‘Future’ of Web Monitoring” Danger Room. *Wired.* Last modified July 28, 2010. http://www.wired.com/dangerroom/2010/07/exclusive-google-cia/?utm_source=Contextly&utm_medium=RelatedLinks&utm_campaign=Previous.

———. “Pentagon Research Conjures Warcraft Terror Plot.” Danger Room. *Wired.* Last modified September 15, 2008. http://www.wired.com/dangerroom/2008/09/world-of-warcra/.

Skelton, Alissa. “U.S. Wants you to Test Terrorist Tracking with Social Media Game.” U.S. and World. *Mashable.* Last modified February 9, 2012. http://mashable.com/2012/02/09/social-media-tracks-terrorists/.

Smith, Josh. “House Panel Decries ‘Chilling’ Effect of DHS Social-Media Monitoring.” Technology. *National Journal.* Last modified February 16, 2012. *l*http://www.nationaljournal.com/tech/house-panel-decries-chilling-effect-of-dhs-social-media-monitoring-20120216.

Snow, Gordon M. “Statement of Gordon M. Snow Assistant Director, Cyber Division Federal Bureau of Investigations Before the House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security.” Last modified July 28, 2010. http://judiciary.house.gov/hearings/pdf/Snow100728.pdf.

Steel, Billy. “Money Laundering – Business Areas Prone to Money Laundering.” Billy’s Money Laundering Information Website. Accessed March 2, 2012. http://www.laundryman.u-net.com/page9_bus_prone_ml.html.

Stokes, Jon. "EFF's New Lawsuit, and how the NSA is into Social Networking." Law & Disorder / Civilization & Discontents. *Ars Technica.* Last modified July 23, 2009. http://arstechnica.com/tech-policy/news/2009/07/effs-new-lawsuit-and-how-the-nsa-is-into-social-networking.ars.

Stonebrook, Martha, S., and Richard A. Stubbs. “Social Networking in Law Enforcement – Legal Issues.” *Americans for Effective Law Enforcement.* Accessed January 4, 2012. http://www.aele.org/los2010_sm-visual.pdf.

Sullivan, Bob. “Would you ‘friend’ a stranger?” *MSNBC,* March 22, 2011. http://redtape.msnbc.msn.com/_news/2011/03/22/6501983-would-you-friend-a-total-stranger.

Symantec. “Symantec Report on Attack Kits and Malicious Websites.” Accessed April 3, 2011. https://scm.symantec.com/resources/b-symantec_report_on_attack_kits_and_malicious_websites_21169171_WP.en-us.pdf.

The Telegraph. “Al-Qaeda Plans to Wage Holy War on Facebook.” December 21, 2008. http://www.telegraph.co.uk/news/worldnews/3885367/Al-Qaeda-plans-to-wage-holy-war-on-Facebook.html.

Treverton, Gregory F. “DHS’s First Year: A Report Card: Intelligence Gathering, Analysis, and Sharing.” Accessed January 31, 2012. http://www.tcf.org:8080/Plone/publications/pdfs/pb451/2.intelligence.pdf

Turner, Michael. “Intelligence and Homeland Security.” Lecture, San Diego State University, San Diego, CA, September 16, 2010.

United Nations Counter-Terrorism Implementation Task Force. “Countering The Use Of The Internet for Terrorist Purposes-Legal and Technical Aspects.” CTITF Working Group Compendium. Accessed March 4, 2012. http://www.un.org/es/terrorism/ctitf/pdfs/ctitf_interagency_wg_compendium_legal_technical_aspects_web.pdf.

United States Army. “OPSEC and Safe Social Networking.” The Official Homepage of the United States Army. Accessed March 3, 2012. https://ia.signal.army.mil/SocialmediaandOPSECbrief1.pdf.

U.S. Government Accountability Office, “Federal Efforts Are Helping to Alleviate Some Challenges Encountered b State and Local Information Fusion Centers,” Homeland Security. *U.S. GAO*. Last modified October 30, 2007. http://www.gao.gov/assets/270/268516.pdf.

Vergel, Gina. “Security Expert: Social Networking Sites are Hotbeds of Terrorism.” *Fordham University*. Accessed February 13, 2012. http://www.fordham.edu/Campus_Resources/eNewsroom/topstories_1916.asp.

Verton, Dan. “Virtual Threat, Real Terror: Cyberterrorism in the 21st Century” *Errata: Dan Verton.* Accessed March 4, 2012. http://attrition.org/errata/sec-co/danverton-02-testimony.html.

VizCenter. “Exercise 24.” *San Diego State University*. Last modified September 24, 2010. http://vizcenter.net/events/exercise-24/.

Warren, Christina. “Revealed: The FBI Wants to Monitor Social Media.” U.S. and World. *Mashable.* Last modified January 26, 2012. http://mashable.com/2012/01/26/fbi-social-media-monitoring/.

Weinberger, Sharon. “Congress Freaks Out Over Second Life Terrorism” Danger Room. *Wired.* Last modified April 4, 2008. http://www.wired.com/dangerroom/2008/04/second-life/.

Wikipedia. “Communications Decency Act.” Last modified April 17, 2012. http://en.wikipedia.org/wiki/Communications_Decency_Act.

———. “Tencent QQ.” Last modified March 30, 2012. http://en.wikipedia.org/wiki/Tencent_QQ.

Williams, Christopher. “Twitter Threatened with Court Over Hezbollah Tweets.” *The Telegraph,* December 30, 2011. http://www.telegraph.co.uk/technology/twitter/8984705/Twitter-threatened-with-court-over-Hezbollah-tweets.html

Wilson, Clay. “Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress.” *CRS Report for Congress.* Last modified January 29, 2008. http://www.fas.org/sgp/crs/terror/RL32114.pdf.

Wolfe, Alexander. “Twitter in Controversial Spotlight Amid Mumbai Attacks.” *Information Week.* Last modified November 29, 2008. http://www.informationweek.com/news/global-cio/interviews/229209104.

Yzaguirre, Mark R. “Drug Cartels get more sophisticated.” *FrumForum.* Last modified January 3, 2012. http://www.frumforum.com/drug-cartels-get-more-sophisticated.