Social Media and the U.S. Army: Maintaining a Balance

A Monograph

by

MAJOR Todd A. Moe

United States Army

School of Advanced Military Studies

United States Army Command and General Staff College

Fort Leavenworth, Kansas

AY 2011

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
28-04-2011	SAMS Monograph	June 2010 – April 2011

4. TITLE AND SUBTITLE
Social Media and the U.S. Army: Maintaining a Balance

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Major Todd A. Moe (U.S. Army)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
School of Advanced Military Studies (SAMS)
250 Gibbon Avenue
Fort Leavenworth, KS 66027-2134

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Command and General Staff College
731 McClellan Avenue
Fort Leavenworth, KS 66027-1350

10. SPONSOR/MONITOR'S ACRONYM(S)
CGSC

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Now that the Department of Defense has permitted the use of social media for both private and official purposes, the question becomes, can the military, the Army in particular, obtain the benefits sought from social media use without seriously compromising individual and operations security? Answering this question required an initial assessment of Army goals and objectives to determine why the Army risked the use of social media, which revealed two reasons immediately. First, the Army needed social media to communicate its inform and influence activities more effectively. Second, social media was the primary means by which soldiers maintained contact with their friends and family and, consequently, became a significant element in maintaining soldier morale. If the Army did not need social media to distribute its inform message, it might have avoided the difficulties created by the personal use of social media by soldiers. Thus, the security risk posed by the use of social media cannot be reduced to a simple enforcement of operations security rules. Nevertheless, soldiers who are not trained to avoid the disclosure of classified or sensitive information will, through their ingrained habits, present a significant security risk. Bottom line, all military personnel require training on appropriate use of social media now.

15. SUBJECT TERMS
Social Media, New Media, Geotagging, Inform and Influence Activities, Strategic Communications, Operations Security, OPSEC, Risk, Privacy, Facebook, Personal Identifiable Information, 1st Amendment, UCMJ, Social Media Handbook, Smartphone, Internet, U.S. Army

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
					Wayne W. Grigsby Jr. COL, U.S. Army
a. REPORT (U)	**b. ABSTRACT** (U)	**c. THIS PAGE** (U)	(U)	(U)	**19b. TELEPHONE NUMBER** *(include area code)* 913-758-3302

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

MAJOR Todd A. Moe

Title of Monograph: Social Media and the U.S. Army: Maintaining a Balance

Approved by:

_____ Monograph Director
William J. Gregor, Ph.D.

_____ Second Reader
Cliff Weinstein, LtCol, USMC

_____ Director,
Wayne W. Grigsby, Jr., COL, IN School of Advanced Military Studies

_____ Director,
Robert F. Baumann, Ph.D. Graduate Degree Programs

Abstract

Social Media and the U.S. Army: Maintaining a Balance by MAJOR Todd A. Moe, U.S. Army, 37 pages.

Now that the Department of Defense has permitted the use of social media for both private and official purposes, the question becomes, can the military, the Army in particular, obtain the benefits sought from social media use without seriously compromising individual and operations security? Answering this question required an initial assessment of Army goals and objectives to determine why the Army risked the use of social media. The assessment revealed two reasons. First, the Army needed social media to communicate its inform and influence activities more effectively. Second, social media was the primary means by which soldiers maintained contact with their friends and family. Consequently, social media has become a significant element in maintaining soldier morale. If the Army did not need social media to distribute its inform message, it might have avoided the difficulties created by the personal use of social media. Thus, the security risk posed by the use of social media cannot be reduced to a simple enforcement of operations security rules. Nevertheless, soldiers who are not trained to avoid the disclosure of classified or sensitive information will, through their ingrained habits, present a significant security risk.

To understand the situation and to derive the needed training required an initial examination of social media as a means of communications. That discussion along with a discussion of personal soldier use reveals that social media supports the Army inform and influence activity requirements, but introduces the risk of spillage through social media. In other words, soldiers have habits that create vulnerabilities that enemies of the United States can easily exploit. An examination of casual social media use revealed common practices that stand contrary to sound operations security. Comparing social media habits with regulatory requirements produced a list of key elements of required training.

The reality is that evolutionary information changes will continue without the military's consent. All military personnel require training on appropriate use of social media now. The Army can institute training that raises awareness of these dangers for all service members. Ideally, social media will become a manageable medium with which to communicate the right messages and maintain good order and discipline within the Armed Forces.

Table of Contents

Table of Figures

Introduction

Imagine what a soldier in World War II felt, thought, and wrote back to his loved ones. He wrote about unglamorous soldiering on cold mud, his worries and aspirations, the enemy, and loneliness. He might have written about who 'bought the farm' or how green and young the individual replacements look. He would express all this in a letter that would go to the company clerk. After that point, the letter's content was edited or censored. What the family received on the far end was a note encompassing many of the same emotions but possibly lacking the details that conveyed the actual events as they unfolded. Lyle S. Wessale was an 18-year-old draftee, serving in Europe in 1944 when he wrote the following passage to his family:.

> Please don't worry about me. I came out of the battle unscratched. All I can say or do is get on my knees and pray to God for thanks and for being with me. You can't help but think about the fellows who were unfortunate as my buddy was. I try to forget about him but it is hard.

That letter had more details, but Army censors tore off portions of the pages. The soldier finished with a compelling thought: ″I almost broke down from the strain and lack of sleep but stuck it out.″[1]

In today's 2011 modern information environment, social media creates new security risks unlike those seen in the past. Social media has changed the face of personal privacy in society and has the potential to undermine operations security. Recently, it was believed that two Navy sailors (Petty Officer Newlove, a 25-year-old from Renton, Washington, and Petty Officer 2nd Class Justin McNeley, a 30-year-old from Wheatridge, Colorado) were captured by Taliban insurgents in Afghanistan. The Navy was concerned that the news media and Taliban would exploit the sailors' Facebook profiles. Major Juanita Chang, Director of Online and Social Media in the Office of the Chief of Public Affairs, gave a personal account of how the U.S. Navy asked her to

[1] Vincent Pierri, "Letters from the front chronicle a World War II soldier's ordeal," http://www.dailyherald.com/story/?id=384105 (accessed September 31, 2010).

help take down the Facebook profiles of the two sailors.[2] In this case, the Army on the Navy's behalf made an urgent request to Facebook administrators who voluntarily took the profiles off-line. This kind of forward and fast thinking is an excellent example of proactive operations security in today's new media environment. Information now moves at rapid speed and requires non-traditional approaches and techniques to manage it. The Army and social media are in a transitional stage. The rules and regulations that govern the Army's social media use require refinement and in many cases complete revision.

In February 2010, the Department of Defense issued a memorandum, DTM 09-026, that changed the social media usage policy. The memorandum permitted military personnel to access social media on unclassified Internet networks. However, the policy still prohibited gambling sites, forums that encourage hate speech and racism, and pornography websites on government networks. Some examples of newly authorized services:

- Social networking services (e.g., Facebook, MySpace, Twitter.)
- Image-and video-hosting Web services (e.g., YouTube, Flicker.)
- Personal, corporate, or subject-specific blogs
- Similar collaborative, information sharing-driven Internet-based capabilities users are encouraged to add and/or generate content

The Department of Defense (DoD) is setting a new precedent by allowing the use of social media websites by its personnel and on its networks. This new policy may have a dramatic impact on the flow of information in and out of the military establishment. Deployed soldiers who use military networks to maintain contact with families and friends, most commonly use social media. In a change of direction, DoD now subscribes to the use of social media as a tool and cites an example like the aftermath of the earthquake in Haiti as one of several reasons to adapt. In Haiti, social media sites like Facebook and Twitter acted as conduits to broadcast news, coordinate relief efforts, and raise donations.

---

[2] Juanita Chang, interview by author. Fort Leavenworth, KS, August 30, 2010.

Given that military personnel now have access to social media on a regular basis, the military absorbs the risk that someone will reveal information about critical missions that must remain secret.[3] A soldier can "tweet" or update his Facebook status for the world to see in a matter of seconds without anyone censoring his message, which is significant because once the information is on the internet it cannot be erased. While social media permits soldiers to feel a greater connection to family and friends, it also allows others on the World Wide Web to access their personal information which could potentially impact operations security. There are certain types of information found within social media that place soldiers at risk. "Due to the rapidly evolving information environment, with pervasive media coverage and the democratization of instantaneous global communication technology, messages, generated at the tactical, level can quickly reach mass audiences and have potential strategic implications."[4]

At one time, the adage 'mind your own business' aptly reflected the average American citizen's feelings about personal privacy, but views have changed. The growing phenomenon of social media has all but eliminated personal privacy. Today's troops do not have the same sense of privacy that would cause them to think twice before posting personal information. Soldiers born after 1980 have grown up using technology like social media. Social media permits people to share online details about their lives, their associates, their families, their political and even their religious beliefs. Everything ranging from what was eaten for breakfast to instantly uploaded photos with GPS geotagging is open for public viewing.[5]

---

[3] Raj Dash, "Does Social Media Compromise Military Operations?" http://www.socialtimes.com/2010/03/does-social-media-compromise-military-operations (accessed March 28, 2011).

[4] Lee Bokma, "Strategic Communication for Tactical Leaders" (master's thesis, Fort Leavenworth: Command and General Staff College, 2010), 5.

[5] Kate Murphy, "Web Photos That Reveal Secrets, Like Where You Live," http://www.nytimes.com/2010/08/12/technology/personaltech/12basics.html (accessed March 5th, 2011). A geotagged photograph is a photograph which is associated with a geographical location by embedded data. Usually this is done by assigning at least a latitude and longitude to the image, and optionally altitude, compass bearing and other fields may also be included.

Now that the Department of Defense has permitted the use of social media for both private and official purposes, the question becomes, can the military, the Army in particular, obtain the benefits sought from social media use without seriously compromising individual and operations security? Answering this question required an initial assessment of Army goals and objectives to determine why the Army risked the use of social media. That assessment revealed two reasons immediately. First, the Army needed social media to communicate its inform and influence activities more effectively. Second, social media was the primary means by which soldiers maintained contact with their friends and family and, consequently, became a significant element in maintaining soldier morale. If the Army did not need social media to distribute its inform message, it might have avoided the difficulties created by the personal use of social media by soldiers. Thus, the security risk posed by the use of social media cannot be reduced to a simple enforcement of operations security rules. Nevertheless, soldiers who are not trained to avoid the disclosure of classified or sensitive information will, through their ingrained habits, present a significant security risk.

To understand the situation and to derive the needed training requires an initial examination of social media as a means of inform activities. This discussion is made more intelligible if, while discussing social media in the inform and influence context, important definitions of social media and its components are also addressed. The discussion of personal soldier use supports the Army inform and influence activity requirements, but introduces the risk of casual use of social media. In other words, soldiers have habits that create vulnerabilities that enemies of the United States can easily exploit. An examination of casual social media use reveals common practices that stand contrary to sound operations security. Comparing social media habits with regulatory requirements reveals the key elements of required training.

Inform and Influence Activities, Social Media, and Definitions

What are inform and influence activities? In 2011, *strategic communication* was renamed *inform and influence activities*. Consequently, the Army has only recently started to rewrite its doctrine to reflect this change. In FM 3.0 Change 1, the Army uses inform and influence activities to focus efforts of soldiers to understand and engage specific audiences. Inform and influence activities create, strengthen, or preserve conditions favorable for to Army's interests, policies, and objectives. The Army does this by constructing the message to influence the will of the target audience. Ideally, inform and influence activities will strengthen the will of a friend and weaken the will of the enemy. Understandably, inform and influence activities are very important. The U.S. Joint Forces Command (JFCOM) has stated that "victory in the long war ultimately depends on strategic communication by the U.S. and its partners."[6] The information communicated by inform and influence activities is vital to US success in current and future conflicts. However, in the context promoted by JFCOM, inform activities are meant for use by public affairs, public diplomacy, and information operations professionals only. A conservative military culture seeks to control every detail that is released about the organization. Social media breaks the paradigm of the regimented control the Army works to maintain – the Army no longer has control over the entire message. Access to social media provides the means for the full spectrum of the force – from the senior leader to the private – to communicate to the world and, thereby, obtain overwhelming benefits and sometimes, dangerous ramifications. The Army's Chief of Public Affairs Major General Stephen R. Lanza stated that it takes more than a press release to

[6] U.S. JFCOM Joint Warfighting Center, *Commander's Handbook for Strategic Communication and Communication Strategy* (Suffolk, VA: USJFCOM Joint Warfighting Center, 2009) under "Commander's Handbook for Strategic Communication and Communication Strategy," http://www.carlisle.army.mil (accessed November 9, 2010), I-1.

successfully communicate.[7] Effective communication requires an aggressive effort to tell the Army story. Engagement with different audiences requires alternate ways to inform the public across a variety of platforms. It also requires monitoring of social media to understand what is being said, both online and through traditional media. To remain relevant in this new information domain, the Army embraced social media.

So what is social media? *Social media* is a subset of the *new media* information environment within which the military now operates. The Army, as a service, has defined social media as "dialogue-based web platforms, sites such as Facebook, MySpace, Flickr, YouTube, and Twitter."[8] These services provide a medium for sharing experiences and unfiltered information, "putting the ear of the world to the lips of anyone who wishes to speak."[9] *New media* is defined as digitized information found and accessed on the Internet from any electronic device. The Air Force distinguishes between new media and social media. New media is as the "emergence of digital, computerized, or networked information and communication technologies; while social media defines the various activities that integrate technology, social interaction, and the construction of words, pictures, videos and audio."[10] The shift to social media changes the way that soldiers communicate and share details about their daily lives, to include details about work. An effective Army communicator of the latest happenings is no longer simply a trained professional speaking off talking points. The latest information may come from a soldier who was on the front lines via social media.

---

[7] Office of the Chief of Public Affairs, *U.S. Army Social Media Handbook 2011* (Washington D.C.: Office of the Chief of Public Affairs, 2011), http://www.slideshare.net/USArmySocialMedia/army-social-media-handbook-2011 (accessed January 26, 2011), 2.

[8] Office of the Chief of Public Affairs, 5.

[9] Bokma, 6.

[10] Air Force Public Affairs Agency Emerging Technology Division," *Social Media and the Air Force* " (Air Force Public Affairs Agency, 2009), www.af.mil/shared/media/document/AFD-090406-036.pdf (accessed October 23, 2010), 3.

To interact for social and professional purposes, the soldier might use *social networking services* like Facebook and MySpace. Social networking is a phenomenon that has exploded in recent years. Facebook is the largest and most popular social media site in the Western world. The site was originally created in February 2004 by Mark Zuckerberg and his college roommates and a handful of fellow computer science students at Harvard. Originally Facebook provided services for only Harvard students. However, later it expanded to any university students, then to high school students and then to anyone over the age of 13. By July 2010, Facebook surpassed 500 million active users around the world and continues to grow.[11] Facebook is the largest and most visited social networking site in the world. Facebook cuts across demographics and is popular with all segments of society. An average Facebook user spends over 55 minutes per day surfing the site (See Appendix A).[12] Facebook is second only to Google Inc. in page visits per day. This new internet phenomenon is changing how people think about, gather, and share their personal information. The Army considers social media as the standard for spreading information. With the liberalization of social media use comes the risk that soldiers will release sensitive or classified information. Therefore, soldiers need to understand the associated risks of using the various social media platforms.

Typically, social networking websites allow users to upload a *profile* that allows the user to display as little or as much detailed data as they like. This *profile data* can include information about the user's family, birthday, where the user lives, place of birth, religious views, schooling, and professional experience. Much of this information is analogous to personally identifiable information (PII) which, in other business and government environments, is protected by law. Existing security regulations do not address social media directly, but information released

---

[11] Facebook Inc. "Facebook Press Room," http://www.facebook.com/press/info.php?statistics (accessed March 20, 2011).

[12] Muhammad Saleem, "Visualizing 6 Years of Facebook [INFOGRAPHIC]," http://mashable.com/2010/02/10/facebook-growth-infographic/ (accessed February 20, 2011).

through new and emerging social media use is governed by Army regulations. The government and the individual are responsible for maintaining operations security (OPSEC). To protect operations security, the Army wrote AR 530-1. AR530-1 addressed concerns about using the Internet and mentions some emerging social media activities like weblogs (blogging). The regulation defines operations security as a process to deny potential adversaries information about capabilities and intentions by identifying, controlling, and protecting unclassified information that gives evidence of the planning and execution of sensitive activities.[13] All Army personnel are required to practice safe OPSEC in performance of daily duties. Operations Security is meant to become second nature to personnel during work and home life. The regulation also addresses family members and the role they play in protecting information about their soldier. The regulation also places a requirement on the user to use proper judgment to ensure OPSEC after receiving appropriate guidance and awareness training. While the Army cannot mandate that family members adhere to OPSEC procedures, the regulation simply asks that military family members be aware of OPSEC to help safeguard potentially critical and sensitive information. OPSEC procedures protect the soldier and prevent his compromise during present and future operations.[14]

Although AR 530-1 does not address social media directly, the regulation does address new technology (circa 2007) such as the internet and blogs. It emphasizes that adversaries are looking for seemingly useless open-source information, which is not classified, but can be pieced together like pieces to a puzzle. With enough of these pieces of information, the enemy can create a snapshot to attain a greater understanding of the bigger environment and possibly learn something useful to use against the Army. Maintaining OPSEC transcends its traditional role of

---

[13] Interagency OPSEC Support Staff, *National OPSEC Program*, https://www.iad.gov/ioss/department/opsec-glossary-of-terms-10026.cfm (accessed February 14, 2011).

[14] Michael Hampton, "Army: "Soldier blogging unchanged" in new OPSEC regulation," http://www.homelandstupidity.us/2007/05/03/army-soldier-blogging-unchanged-in-new-opsec-regulation (accessed March 25, 2011).

upholding security. Operations Security is more than the marking, handling, and classifying of information. It is different from traditional security in that the Army wants to eliminate, reduce, and conceal indicators, and unclassified and open-source observations of friendly activity that can give away critical information.

The regulation clearly states that commanders are responsible for implementing OPSEC. Commanders are required to ensure that their personnel understand what is critical and sensitive information and how to implement procedures to protect it. Although the regulations do not directly address social media, commanders have the authority to enact local regulations that have requirements in AR 530-1. The regulation assumes that the command has a better grasp of how social media is used in local environment. The concern becomes whether individual commands have the requisite tools to leverage social media and safeguard information at the same time.

A demographic and cultural shift complicates the use of social media. Director of Online and Social Media for the U.S. Army, Major Juanita Chang has experienced this cultural shift firsthand. While working in the Pentagon, she encounters "the nonbelievers, who believe that social media is just something that teenagers and celebrities use."[15] Generational differences uncover different perceptions of social media and the need to share personal information. The gap is evident between young soldiers and their older leadership. John Palfrey and Urs Gasser defined digital immigrants and natives in their book, *Born Digital: Understanding the First Generation of Digital Natives*. *Digital natives* are people born into the digital environment after 1980. Digital natives have distinct understanding of their relationships to information technology, their definitions of privacy, and forms of interaction.[16] *Digital immigrants* are people who embrace new digital technologies like the Internet, but were born prior to 1980. *Digital illiterates* "are still

---

[15] Alex Salta, "Conversations with Communicators: Juanita Chang, U.S. Army," http://ohmygov.com/blogs/general_news/archive/2011/03/11/conversations-with-communicators-juanita-chang-u-s-army.aspx (accessed March 24, 2011).

[16] John Palfrey and Urs Gasser, *Born Digital: Understanding the First Generation of Digital Natives* (New York: Basic Books, 2008), 4-7.

many people in government -- especially higher up in government," writes one group of strategic experts, "who have little experience with new communications and information technologies and [sic] avoid using them."[17] Therefore, the people who establish training and internet protocols for the common soldier are often completely unaware of the power of this new world of information. Given that digital natives have a different view of personal privacy, allowing individual soldiers to determine the accessibility of information online can be hazardous to the mission at hand. Collectively, digital natives have grown up with patterns of behavior that run contrary to regulated operations security practices. Given this reality, is this farcical statement satirizing an Army study of issuing every soldier a smartphone off the mark? "A sudden increase in US soldiers being picked off by enemy snipers, has led the US Army to ban the use of Google Latitude, Facebook Places and Foursquare on government issued smartphones."[18] In all likelihood, digital natives will not think twice about sharing information like pictures with geotags, real-time location, and blogging personal details about their lives.

The digital native was born to a world in which his personal information is collected by outside parties and viewed as a commodity. While internet privacy is the ability of the individual to control what information he reveals about himself over the Internet, and to control who can access that information, the use of social media leads to the inevitable conclusion that there is reduced privacy when the Internet is involved. Because of the increased use of social media, there is the increased ability to gather, send, and aggregate information about an individual or organization. So, personal information displayed in social media should receive thoughtful

---

[17] Steven R. Corman and Jill S. Schiefelbein," Communication and Media Strategy in the Jihadi War of Ideas" *Arizona State University.* (2006), http://www.asu.edu/clas/communication/about/terrorism/publications/jihad_comm_media.pdf (accessed December 8, 2010), 86.

[18] Joseph L. Flatley, "US Army Connecting Soldiers to Digital Applications program putting smartphones in soldiers' hands this February," http://www.engadget.com/2010/12/14/us-army-connecting-soldiers-to-digital-applications-programs-put/ (accessed March 23, 2011). Google Latitude, Facebook Places and Foursquare are location-aware applications in smartphones that allow users to check into specific places and share their location with their friends.

consideration prior to posting because the *viral* nature of the Internet allows information to spread rapidly within the social media ecosystem. Once sensitive information finds its way onto the Internet, it becomes nearly possible to reclaim the information. The U.S. government's failed attempts to squash the release of damaging classified information through Wikileaks proves the point.[19]

A website called Socialnomics – The Social Blog helps to bring perspective to the emergence of social media, its importance to society, and its pervasiveness into the average digital immigrant and native lifestyle.[20] Socialnomics put together a few basic facts to demonstrate the global reach of social media:

- 96 % of people in Generation-Y (Digital Natives) have joined a social network.
- Social media has overtaken pornography as the #1 activity on the web.
- Consider the time it took for previous media forms to reach 50 million users:
    - Radio: 38 years, TV: 13 years, Internet: 4 years, iPod: 3 years
    - Facebook added 100 million users in 9 months
- If Facebook were a country, it would be the 4th largest in the world, behind China, India, and the United States. Yet, China's Q-zone (Chinese language social networking site) is larger than Facebook.
- 80% of Twitter usage is on mobile devices.
- YouTube is the second largest search engine in the world, they hold over 100 million videos.
- 24 of the 25 largest newspapers in the US are experiencing record decline in circulation.

This points to decline in traditional media and increase in social media. Statistically by age group, 65% of the Army population belongs to the Digital Native generation. To digital natives and immigrants, social media is not a fad but a way of life. Thus, the military services must address ever-growing social media use within the ranks.

---

[19] From the website: "WikiLeaks is a non-profit media organization dedicated to bringing important news and information to the public. We provide an innovative, secure and anonymous way for independent sources around the world to leak information to our journalists. We publish material of ethical, political and historical significance while keeping the identity of our sources anonymous, thus providing a universal way for the revealing of suppressed and censored injustices."

[20] Erik Qualman, "Social Media Revolution Video (Refreshed)," http://www.socialnomics.net/2010/05/05/social-media-revolution-2-refresh (accessed October 12, 2010).

Craig Willis, an associate professor at Massachusetts' Worcester Polytechnic Institute, pragmatically stated that any picture, any piece of personal information made available to these [social media] sites, takes control of the content away from the individual. "If there's something you would rather an employer or future employer or someone else down the line not to know about, unless there's a real need to [share it], my clear advice is to not."[21]

Evan Noynaert, assistant professor of computer science at Missouri Western State University, said the cynic in him believes that every Facebook user is compromised to some degree.[22] Understand that when personal information resides on a public server, that information is at the mercy of that business entity. Most people do not understand the business model that enables Facebook and third-party applications to make money by providing social networking services. They are not providing a free service to allow an individual to network innocently. They are looking for ways to make money from that information, mainly by selling it.

Individual concepts of privacy vary by generation. Often, the twenty-something person's concern pertains only to keeping his activities from his parents' view. Facebook founder Mark Zuckerberg stated this another way, "we view it as our role in the system to constantly be innovating and be updating what our system is to reflect what the current social norms are."[23] An executive director for the World Privacy Forum, Pam Dixon believes that people really do want to share their information and have the right to share as much as they please. She also goes on to warn that disclosure of information has a possibility for misuse in certain situations. Dixon warns that, in an attempt to make money, businesses may consider privacy of secondary importance.

---

[21] Lucy Soto, "Not-so-private Web: Information leaks on social networks can leave users vulnerable," *The Atlanta Journal – Constitution* (February 14, 2010): B.1.

[22] Jimmy Myers, "Some worry about social networking sites: Expert: Third-party applications may put users at risk," *McClatchy-Tribune Business News* (November 30, 2009).

[23] Joan Goodchild, "10 Security Reasons to Quit Facebook (And One Reason to Stay On)," http://www.csoonline.com/article/print/584813 (accessed August 18, 2010).

Employers are already searching social networks to help them determine whether prospective employees fit into their corporate culture. However, on Facebook, Dixon said, employers can find information about race, gender, and marital status, information that fair-employment laws prohibit employers from seeking outright. Potential employees are unwittingly exposing themselves to discrimination in hiring, and they will most often never know what happened.[24]

It is not surprising that in May 2010 a movement was started within Facebook for users to quit Facebook. The movement was a reaction to poor privacy security controls within Facebook. In the end, the movement failed to generate much buzz outside of media channels. Facebook users did not quit Facebook en mass as some experts predicted. Compared to the 500 million (and growing number of) users currently using Facebook, the tens of thousands of users that quit amounted to essentially a meaningless demonstration of user dissatisfaction with the Internet giant. In the end, a majority of users see more benefits with social media than risks. The lack of privacy was not enough to deter use. The Army, however, cannot afford to be so unmindful of the dangers and links between soldier privacy and operations security. In civilian life, a violation of a person's internet privacy and data may result in a hassle like identity theft. In the military, however, violations of internet privacy can threaten more than identity and credit score. It puts lives at risk.

The exploitation of personal data is not a phenomenon applicable to only Facebook. During basic Web use, computers track user movements from website to website and routinely glean and collect information. Companies use this information to build and share profiles with user names, friends' names, shopping habits, and other personal information. Numerous entities (business and government types) track unknowing and unwilling individual users. "Someone, other than the government, has a honking-great database on me. And that probably means that

---

24 Benny Evangelista, "Too much sharing online?" *San Francisco Chronicle* (December 30, 2009): DC.1.

they have a similar amount of data on you, Dear Reader," blogged Roger Thompson, a chief research scientist with software security company AVG. [25] Is the solution to avoid these activities altogether? Some people believe, like Pete Cashmore, the founder of Mashable.com, that social networking is required to stay relevant and connected in today's connected world. In an opinion piece on CNN.com, he wrote that professionals must choose to either share online or "fade into lonely obscurity." Conversely, he also wrote, "Privacy is dead and social media holds the smoking gun." So if social media is an unstoppable train that people need to be on to further their professional and personal interests, how do individuals control the threats to their personal security? Even more important, how does the Army control the threats to operations security?

The Soldier's Role in Inform and Influence Activities

Adversaries of the United States use traditional and social media mediums to their advantage. As reported in Military Review article, *Learning to Leverage New Media*, Hezbollah used several means including its own satellite channel, Al Manar, to reach to some 200 million viewers within the region. New media provided a "direct link between Hezbollah military activities…and viewers, Al Manar timed coverage of spectacular tactical actions for maximum strategic effect." In one instance, Hezbollah recorded an anti-ship missile attack on an Israeli naval destroyer Hanit and claimed to have sunk her. Immediately video of this incident spread on traditional media (HezbollahTV) and subsequently went viral by way of YouTube. The Israeli Defense Forces (IDF) took *over 24 hours* to respond to the report of the attack on their ship and refute the claims about her sinking. In this situation, Hezbollah used information as a strategic weapon in a kinetic fight. "Hezbollah continued to use self-justifying and self-congratulatory information to affect perceptions of blame, responsibility, and victory."[26] As other organizations

[25] Soto, B.1.

[26] William B. Caldwell IV, Dennis M. Murphy, and Anton Menning, "Learning to Leverage New Media: The Israeli Defense Forces in Recent Conflicts," *Military Review*, 2009: 2-10.

take advantage of new media to spread their agenda, the Army must also use this tool. The example of Hezbollah demonstrates just how powerful these methods are as a means to inform and influence. If left unanswered, such messages spread like wildfire and negatively influence military efforts by swaying domestic and international public opinion.

Using social media channels allows the Army to perform information activities and reach out to a vast audience. Many people may not understand the military, who we are, and why we do what we do. The Army can use these new forms of media to dispel popular myths regarding the military and increase goodwill towards its members. In an internal report for the Assistant Secretary of Defense for Networks and Information, Roxie Merritt set forth eight reasons why new media tools are crucial to the mission (see Appendix B).[27] First, the Army wants to use new media to share information with the American public in a timely manner. U.S. Ambassador Richard Holbrooke famously quipped, "How can a man in a cave out-communicate the world's leading communications society?" Critics would say the government and the Army are not up to the task in the post-9/11 new media environment. The US government's former reliance on traditional media does not demonstrate the dynamism required to operate in this evolving space. A completely new media strategy is needed where social media is concerned. The operational reality is that social media is becoming a major focus of US Forces-Afghanistan (USFOR-A) communication efforts. In Afghanistan, USFOR-A rapidly delivers an unfiltered view of the war from troops on the ground, and is opening a two-way dialogue with people around the world interested in the Afghanistan mission. The USFOR-A provides a firsthand look at reports, videos, and images from troops. These products are posted prior to media release on US Forces - Afghanistan Facebook page and YouTube. This leads to the second reason the Army uses social media.

---

[27] Roxie Merritt, *DoD Access to Social Media and Social Networking Sites* (Washington D.C.: OASD Public Affairs, 2009), 1.

The Army uses social media to prevent and counter misinformation and disinformation. The military finds an urgent need to maintain a presence in this strategic area because to do otherwise would give free reign to U.S. enemies. U.S. enemies spread their interpretation of events as the events unfold, and now U.S. commanders on the ground use social media to push information to the public as quickly as possible to preempt extremist propaganda. A common generalization worth noting is that an average soldier's unpolished opinion is trusted more than a statement made by a military spokesperson. The average soldier lacks an agenda, which makes him genuine. USFOR-A is most likely following that same line of thought, using online social networking activities to prevent militants from influencing the international press.

Third, social media gives the Army an alternative means to push the message out over traditional media outlets, which prevents the outlets from filtering the message. On a strategic level, the Army uses social media as a tool to communicate the Army's planned message directly to the public. Social media provides the Army another tool that, like a press release, bypasses the filter of mass media outlets like journalists and major television networks. The success of any organization is measured by its ability to communicate, not only internally but also externally. Fourth, the Army relies on a social media's strength to reach out to a distributed audience. By its very nature the dynamics of social media circumvent traditional channels. Throughout history, public opinion has had a strong impact on America's ability to stay the course of military action. Traditional media outlets, such as television and newspaper, are no longer effective as the sole means of shaping how the country perceives the military. When information is incomplete, the Army's reliance on the traditional media for setting the agenda is inappropriate. Social media gives the Army the ability to spread its message to a mass audience and remain independent from entities outside the chain of command who are trying to control the dialogue.

The fifth reason for using social media, posed by Roxie Meritt, relies on the service member's interaction with social media to spread the Army's message. The widespread ability to use social media is a demonstration of senior leader trust in the service member. Inform activities

conducted through social media differ from the concepts enunciated by advertising innovator Edward Bernays in 1928. Edward Bernays described the virtues of effective discourse as a "consistent, enduring effort to create or shape events to influence the relations of the public to an enterprise, idea, or group."[28] However, Bernays envisioned the message being spread by celebrities and prominent figures. In this manner, the public's perceptions are shaped by their observations of strategically positioned spokespersons. In contrast, it is the Army's belief that servicemembers who are armed with a little guidance make the best ambassadors and are the most vocal advocates for the military. The aggregate voice of service members using social media puts forth a positive message that overcomes negative news.

Sixth, the Army wants to use social media to improve transparency and customer service. Transparency shows the institution's commitment to engage with public at large. The Army interacts in a public forum via social media and demonstrates how the government is responsive to the taxpayer's customer service needs. Social media permits two-way dialogue, which provides a platform for the Army to promote and participate in public discourse. These interactions create impressions that have a cumulative effect on how people perceive the military. Social media helps the military participate in the creation of the overall narrative. The narrative is assembled by users when they create and search for information to deepen their understanding and knowledge, and develop their own interpretations of what transpired. Their interpretations become part of the narrative that is shared with others. The final reason for participation in social media is the ability to monitor public opinion. If unfavorable opinions about the military are left uncorrected or unanswered, the Army as an institution loses credibility and disappoints the public's expectations. Thus, the Army must take an active role in monitoring American and world opinion. Consider this practice a form of reputation management. After gauging the current state-

[28] Edward Bernays, *Propaganda* (New York: Horace Liveright Publishing, 1928), 52.

of-affairs, the Army should continue the process of engagement through purposeful and professional interactions with the public.

For the first time in history, the average soldier now has unparalleled access to a wide audience through social media. The Army views the positive aspects of social media as more compelling than the possible dangers of using it. In what kind of environment must a soldier operate within social media? How much control does the soldier have over his environment? Is the ability to control social media a myth?

Social Milieu of the Soldier

The Army is at a critical juncture. Social media has unprecedented access to soldiers and unclassified networks. However, Army policies and procedures in place to safeguard operations security and soldier privacy are outdated. It is entirely possible that in the future, a person's "status" could compromise a whole unit. Soldiers and leaders need to know about the dangers, and need training to counter the risks that social media poses to the armed forces.

> Our adversaries are trolling social networks, blogs and forums, trying to find sensitive information they can use about our military goals and objectives. Therefore, it is imperative that all Soldiers and Family members understand the importance of practicing good operation security measures. [29]

There currently exists no comprehensive social media DOD policy related to online communications and engagement. No current instruction exists to dictate the use of internet-based capabilities. The Navy, Air Force, and the Army have published handbooks that highlight best practices and establish guidelines. The handbooks provide common sense checklists for using social media. However, these handbooks are not regulations; consequently, the handbooks do not govern and promote appropriate use and behavior.

America's adversaries come is several different forms. The first form that comes to mind is the *non-state actors* like Al Qaeda and Hezbollah. The non-state actors are also using social

[29] Office of the Chief of Public Affairs, 4.

media as a cheap and inexpensive means to spread their narrative. Second on the list are *nation-states*. Nation-states have conventional military forces and intelligence services that attempt to glean as much information they can from inexpensive open-source information outlets rather than use the more costly human intelligence collection systems. Chinese hackers and Russian spies dominated media headlines for much of 2010 and clearly demonstrated a real threat. Another threat is the *criminal hacker* who exploits individual privacy data to conduct identity theft, financial gain, or some other criminal purpose. The last threat is the *insider*. The best recent example is Private First Class Bradley E. Manning. This soldier is accused of releasing half a million classified documents to WikiLeaks.

At first glance, the information posted on the average social media site like Facebook appears to be nothing more than harmless details shared with the online world. In actuality, the easily accessed information found within the average user profile makes the individual more susceptible to violations of privacy. A violation of the user's privacy means there is information at risk for exploitation. Users commit common mistakes when they use social media. Oftentimes, the user himself is to blame for compromising his privacy. By extension, social media has placed the military in a similar position where there is a greater chance for spillage of secret information. Without training, it is imprudent to think that a service member would act any differently. Military personnel, like the American public, commit many of the same mistakes. The 'Habits and Hazards' portion of this research will detail several common mistakes. Increasingly, secure personal privacy is becoming nothing more than a historical footnote. Likewise, secrecy is nothing more than a special category of privacy.

Habits and Hazards

It appears the adoption of social media as a communication tool will increase among business and government agencies. Army leadership apparently sees this development as a sign to allow digital users the ability to use social media. The most obvious benefit of social media use is

the morale building benefit of maintaining contact with family and friends. When 65% of 2.6 million military service members are digital natives, they are accustomed to using new media technologies. The same digital natives will continue to grow as a population, and out of habit will expect to use their mobile technologies when they deploy. Digital users have a common set of practices, including the amount of time they spend plugged-in to digital technologies, their tendency to multitask, and their tendency to express themselves and relate to the outside world using some form of social media.[30] They will also expect the same two-way communications to contact their friends and families and access to social media. Digital natives are accustomed to constant electronic contact with loved ones while at home, and being able to extend that privilege on deployment directly affects their emotional well-being. Although it cannot be easily quantified, frequent communication supports the morale of the individual soldier. This is arguably the single greatest rationale for the use of social networking sites and other forms of new media within the Army.

During social media use, friends and family influence the operations security of the service member. Friends and family are part of that two-way communication equation. Laurie Dunlop, an internet marketing expert and military spouse, wrote an article called *When It Comes to Social Media, the U.S. Army Says, "Have at it!" Just Remember OPSEC 101*. She noted that with a quick survey of Facebook status updates, that are freely available on the Internet, she found three (not so) obvious examples of OPSEC violations committed by friends and family members of military personnel in a matter of minutes. Ms. Dunlap deleted specific unit names.

> Butch xxxxx "just wanted to say again, my son is leaving for Iraq, Friday his birthday, to help defend our country and freedom, wishing him and all our men and women to be safe, remember to keep your head down and the power day. let's give mark and all our troops a big HOOAH!——"
>
> Lauren xxxx "I love and miss my soldier who is serving in Afghanistan right now!! I have survived two weeks of this deployment. Just want to say thanks to

[30] Palfrey and Gasser, 4.

> all the soldiers for their service and to the families as well for their love and support!!"
>
> Tami xxxx "Glad I found this site, my son Tony is currently serving with the xxxth BSB, xxx BCT, xx xxxxx xxx, (Fort xx xx) in Afghanistan. I pray every day for his safe return along with his fellow soldiers." [31]

While on the surface each individual posting does not point to a precise description of unit movement times and dates, it could still be useful information to the enemy. The enemy could use movement information to target specific formations and concentrations of soldiers in the air and on the ground. The enemy would then have the means to target their limited assets to get the highest payoff targets. Taken as a whole these entries could piece together a beautiful target for the Army's enemies. Unless friends and family are educated to the dangers, they will continue to violate OPSEC. For the most part, friends and family do not realize that they are doing anything wrong.

The previous example showed how friends and family could very innocently violate OPSEC procedures. By allowing military personnel access to social media, the military is increasing the likelihood that someone will reveal classified information. The Army is placing itself in a position where it will have to play catch-up to protect against similar risks. On 3 March 2010, the New York Times reported that the Israel Defense Forces (IDF) canceled a raid after a security breach via Facebook. It appears that an Israeli soldier updated his Facebook profile, using his cell phone, with details about an upcoming raid on suspected West Bank militants. The soldier wrote, "On Wednesday we clean up Quatanah, and on Thursday, God willing, we come home." Combined with his Facebook profile, the soldier revealed the name of his combat unit, and the time and place of the operation. On the surface, the IDF soldier casually revealed classified information like he was going out for a cappuccino. Fortunately, more security savvy Facebook friends of the soldier noted the breach of operations security and alerted military

---

[31] Laurie Dunlop, "When It Comes to Social Media, the U.S. Army Says, "Have at it!" Just Remember OPSEC 101," http://www.netstrategies.com/blog/web-content/when-it-comes-to-social-media-the-u-s-army-says-have-at-it-just-remember-opsec-101 (accessed January 24, 2011).

authorities. The soldier was court-martialed and sentenced to 10 days in prison.[32] The Israeli military issued a statement:

> Uploading classified information to social networks or any Web site exposes the information to anyone who wishes to view it, including foreign and hostile intelligence services," the military statement read. "Hostile intelligence agents scan the Internet with an eye toward collecting information on the IDF (Israel Defense Forces), which may undermine operational success and imperil IDF forces.[33]

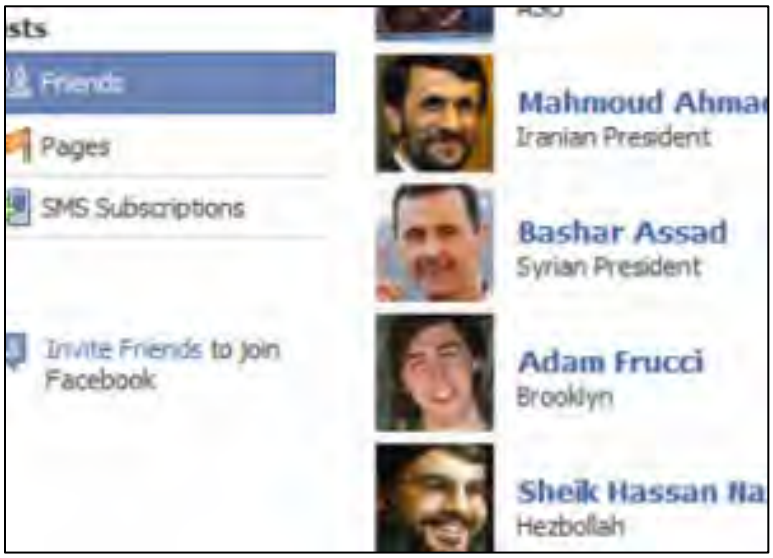

Figure 1 "You think that everyone is your friend?"

IDF soldiers have to understand that their online behavior could directly affect operations, and have deadly implications. To reiterate this point, the IDF also published posters, like the one in Figure 1, of a mock Facebook page showing images of Iranian President Mahmoud Ahmadinejad, Syrian President Bashar Assad and Hezbollah leader Sheikh Hassan Nasrallah with an insightful slogan, "You think that everyone is your friend?"

---

[32]Robert Mackey, "Israeli Raid Canceled After Facebook Leak," http://thelede.blogs.nytimes.com/2010/03/03/israeli-raid-canceled-after-facebook-leak/ (accessed March 10, 2011).

[33] Rubin Shira, "Soldier's Facebook leak forces Israel to cancel raid," http://seattletimes.nwsource.com/html/nationworld/2011249564_isfacebook04.html (accessed March 11, 2011).

In addition to the geographic location revealed through a status update, photos and videos can also reveal a lot. The Army Social Media Handbook asks soldiers to review their photos and videos before posting them online because information gleaned from the background could violate OPSEC. A former Marine, Lance Corporal Briana Moe relates a personal concern for operations security in today's online environment while serving in Uzbekistan in 2003 with an Air Traffic Control Unit.[34] She noticed that it was common practice to take photos while on the flight line to include aircraft, ordinance, and air traffic control equipment, although it was strictly forbidden by regulation. At the time, these actions were viewed as harmless because service members were unable to share their photos until after they got home and printed them. By then, the information was outdated and did not pose a great threat, even though it was still a breach of security. In present-day terms, geotagging cell phones insert the users global-positioning-system (GPS) location data into the electronic signature of a photo or broadcast exact grid coordinates using social networking applications, often without the user being aware of it.[35] Therefore, what may appear to be an innocent photo taken by a Marine and her friends hard at work loading ordinance onto an aircraft, could be disastrous if it were used by a location-based networking application. If other people in the same unit or on the same airfield were to post similar photos, the enemy could compile the images and locations, along with any status updates that leak information, to obtain a full map of where Marines work, sleep, and play. Obviously, Marines would not willingly provide the enemy such information. Nevertheless, they provided the information just the same.

[34] Briana Moe, interview by author, "Concerning Operations Security on Deployment" (February 14, 2011).

[35] Location-based social networking is quickly growing in popularity. Main highlight of these applications is the ability to broadcast the user's geographic location.

Figure 2 Robin Sage's Profile Picture

The Robin Sage experiment showed just how susceptible social media users are, and how little caution they exercise when sharing with "friends" on social networking sites like Facebook. The experiment created a fake profile across several social networking services that managed to snare seasoned military, government, and business world security professionals. Thomas Ryan, co-founder and managing partner at Provide Security, posed as Robin and created a fake profile using a photo of a cute girl (borrowed from an adult website) and gave her a job title 'Cyber Threat Analyst.' Ryan sent requests and established social network ties with more than 300 professionals in the National Security Agency, DOD, and top ranking corporations worldwide. Robin's new friends revealed information that violated military operations security and personal security restrictions. "The worst compromises of operations security I had were troops discussing their locations and what time helicopters were taking off," Ryan said during a phone conversation. People also sought Robin's professional advice, invited her to dinners, and offered her job opportunities. "Not bad in this economy, especially for a person who doesn't even

exist."[36] Security professionals and the average digital native and immigrant alike are subject to these kinds of threats and can be taken in by them. Ryan used geotagging to discern the locations of "several secret military units based on photo metadata found on pictures posted on soldiers' Facebook accounts. He also analyzed connections between military personnel and organizations on social networking websites."[37] Ryan's lesson learned: "Be careful who you choose as your friends."[38] In regards to who a person 'friends' on a social networking site, your friend may not be who he claims to be and conversely, he may not be trustworthy either.

So why did these experts and professionals fall prey to this scam? In their defense, several professionals checked the contact information provided within the fake profile and denied access right away. Yet, overwhelmingly as a group, a digital profile deceived them. With the advent of social media, organizations and experts are still developing rules and guidelines for the safe social media use. In fact, many of these same experts worked at organizations that restricted and banned access to social media on work computers and devices. Yet, many of these professionals were still able to access social media on their personal devices and at home. The digital native will use whatever means are available to him to access social media at home, work, or on a cell phone. Where the user uses social media is not as important as how he uses social media. The individual user requires training to use it safely. In the case of the Army, the personal and professional line is blurring beneath unregulated access to social media.

---

[36] Elliott Fabrizio, "The Dangers of Friending Strangers: the Robin Sage Experiment," Robin Sage Experiment. The experiment created fake Facebook, Twitter and LinkedIn profiles under the alias, "Robin Sage" (accessed October 21, 2010).

[37] Karen Frazier, "Social Media Privacy and the Armed Forces," http://www.reputation.com/how_to/social-media-privacy-us-military (accessed February 15, 2011).

[38] Joan Goodchild, "The Robin Sage experiment: Fake profile fools security pros," http://www.csoonline.com/article/598906/the-robin-sage-experiment-fake-profile-fools-security-pros?page=1 (accessed October 24, 2010).

Regulations and Operations Security

From all appearances, the DoD's training plan for all services is still in the development phase. At a social media conference hosted by DoD in February 2011, a DoD Chief Information Officer representative explained a long-term solution for social media and web policy – a DoD Instruction.[39] The DoD designated this comprehensive policy DoD Instruction 8430.aa. Development of this policy will involve a five-part process: policy creation, policy dissemination, education and training, monitoring for compliance with policy, and compliance enforcement. The DoD has admitted that it is still within the creation stage of development of a long-term strategy for online communications and social media engagement. "Once vetted and approved, the instruction will be a compendium of everything that will be needed for use of Internet-based capabilities – to include content on ethics, operations security, and information assurance."[40] For the Army, social media is here to stay. Timeliness when developing a new policy or changing existing policy needs to be the constant theme and overarching priority. Social media is only going to continue to evolve and grow. The Army cannot afford to ignore the social media phenomenon. The key to success in this time of uncertainty and policy-shaping is to embrace social media, incorporate it into overall tactics through policy and implement an effective training program to manage its use.

Absent definitive guidance from DoD, the Office of the Chief of Public Affairs, Online and Social Media Division published in January 2011, the *U.S. Army Social Media Handbook*. The handbook lays out guidelines on how the military should handle social media services like Twitter and Facebook. The 39-page handbook contains procedures and helpful checklists for commanders and soldiers. These guidelines provide instructions with which to control what

---

[39] Brittney Brown, "The Way Ahead for DoD Social Media Policy," http://armylive.dodlive.mil/index.php/2011/02/the-way-ahead-for-dod-social-media-policy/ (accessed February 13, 2011).

[40] *Ibid*.

information is publicly posted online. The handbook details many common social networking features that can cause a Soldier to innocently reveal a lot about himself. For instance, the handbook strictly states the following:

> Soldiers should not use location-based social networking applications when deployed, at training or while on duty at locations, where presenting exact grid coordinates could damage Army operations. While soldiers are engaged in Army operations, they should turn off the GPS function of their smartphones. Failure to do so could result in damage to the mission and may even put families at risk.[41]

The GPS feature combined with increasing smartphone use is but one example of how social media evolves to incorporate new technologies and new types of interactions. A new feature in social media may have broader security implications not anticipated or detailed in regulation. Therefore, any new feature needs vetting with a wary eye to evaluate if previously mentioned adversaries could use the new feature to compromise privacy and operations security.

MAJ Juanita Chang, Director of Online Social Media Division of the Office of the Chief Public Affairs, gave context to the current Army social media efforts. She is an advocate for social media use that preserves the soldiers' First Amendment rights of free speech and their right to express themselves in a public forum. She paraphrased guidelines put out by her own office. When a soldier is participating in a social networking site on which he or she is or may be identified or associated with the United States Army, the soldier must be very cognizant of how he or she appears to represent his or her organization and the United States of America.[42] The soldier must still uphold OPSEC and Uniform Code of Military Justice (UCMJ) regulations. As a Pentagon insider, she sees a higher number of senior leadership within the military starting to embrace social media. She pointed to Chairman of the Joint Chiefs of Staff Admiral Mike Mullen's use of Twitter and former Army Chief of Staff General George Casey's self-produced YouTube videos, aptly called Chief Cam, as examples of senior leaders using social media. Not

---

[41] Office of the Chief of Public Affairs, 5.

[42] Juanita Chang, interview by author. Fort Leavenworth, KS, September 25, 2010.

surprisingly, most resistance she receives to adopting social media is coming from within the ranks of digitally challenged senior military leadership. She also advocates education, not regulation, to mitigate the risks of social media. MAJ Chang advocates that social media training should start in basic training and carry forward as yearly training for all ranks.

What is on the horizon? By allowing the use of social media, the way the Army communicates with the American public is evolving. In today's media environment, it takes more than press releases to effectively communicate with the public. The social media way of mass communications has added another tool to communicate an organization's message. Social media allows the Army to reach out to many people who may not understand the military, what the Army stands for and why the Army does what it does. It is an Army goal that the military use social media as a way to "lead conversations and participate in stories," thereby telling the Army story to the public by circumventing traditional channels and providing a more comprehensive picture of circumstances on the ground. [43] In an article written in Joint Forces Quarterly, Admiral Mike Mullen wrote, "We must be vigilant about holding ourselves accountable to higher standards of conduct and closing any gaps, real or perceived, between what we say about ourselves and what we do to back it up."[44] The military's failure to live up to promises tarnishes our values. The perception of the services would then be as stereotypical arrogant Americans. This would feed the negative narrative and lose the opportunity to capitalize on a key capability of social media. The military needs to listen and gain greater understanding through building relationships with their stakeholders.[45]

---

[43] Office of the Chief of Public Affairs, 4.

[44] Michael Mullen, "From the Chairman - Strategic Communication: Getting Back to Basics," http://www.jcs.mil/newsarticle.aspx?ID=142 (accessed March 28, 2011).

[45] Ibid.

Essential Training Elements

The Chairman of the Joint Chiefs of Staff places a lot of value in social media's ability to inform the public with a message that is honest and truthful in its portrayal of the military narrative. The average digital native views social media as a mere extension of his personal identity. He grew up in this place. Digital native will go online daily “to experiment with, develop, and learn to represent identity in a space that often feels more private, or at least more controlled, than it probably is." [46] In that context, is the current level of DoD training or individual user experience sufficient to provide the security that DoD requires while exploiting the benefits of social media? Clearly, the answer is no and has two perspectives. The DoD has clear guidelines about operations security, but the weakness in DOD's approach to social media revolves around the piecemeal approach to social media training. As previous examples of common user habits and practices have shown, if users participate in social media unchecked, the potential exists for compromise and “the hamstringing” of military operations in light of ever evolving technology and ever-expanding access.

The Army is operating within the current social media environment without proper systems, policy, and experience to minimize risk. Current regulations that govern operations security provide the guidelines under which the Army operates. However, given the state of rapid change in technology there are no Army regulations written to address social media in its current state; once written and implemented, these regulations would be obsolete. Concerning OPSEC while using social media, this is a leadership and personnel training issue. Existing OPSEC procedures for disclosing any information on a public forum should apply also to social media. How soldiers protect their personal privacy and personal information should be of great importance also. The steps the military takes to develop and inculcate safe social media habits requires a comprehensive and adaptive curriculum. This training will need to address how

[46] Palfrey and Gasser, 27.

younger generation service members normally operate. For a digital native, the personal/professional line is blurred and their instinct is often to share details that DoD would typically guard. A balancing act places faith in the soldier to use this new tool safely and effectively as a means to communicate with the public and his family back home.

This research showed the gaps in user habits and security consciousness that pose risks to operations security. The reality that anything and everything shared online can be accessed by anyone drives the military to demand certainty that no secrets or confidential information are leaked out on sites like Facebook or Twitter. The OPSEC requirement preserves the integrity of information and prevents the adversary from using information to its advantage. The Army should break the norm of business-as-usual and develop new ways to minimize social media risks. The first action the Army needs to take to mitigate the risks of social media is to begin the education process immediately. Education process needs to start as programmed instruction during basic enlisted/officer training and continue through the most senior enlisted and officer schooling. The training focus should revolve around maintaining privacy and operational security when using social media. The families and friends of these soldiers should also be educated. In all likelihood, most Army personnel are using some form of social media or, at least, the digital natives in the ranks are using it frequently. If this is the case, education on these topics becomes the Army's first line of defense.

Second, the proposed education must include simple steps to protect personal privacy. What does it mean to secure your social media privacy settings? While it may seem counterproductive to lock down your social media settings to protect privacy and security, it is still possible to capitalize on the benefits of social networking. Here are five rules to protect online privacy while using the most popular social networking website, Facebook. First, limit the amount of personally identifiable information (PII) contained within the user Facebook profile. Instead of sharing every detail like birth date, street address, contact numbers, and employment history, only place enough information within your profile for someone to connect with you. The

less PII information in your profile the lower the risk of identity theft or accidental exposure of your profile information. Second rule, control the privacy settings of the user profile. Figure 3 illustrates how most social networking sites like Facebook allow the user to control the privacy settings of the user profile. Using Facebook as an example and following the advice found in the Army Social Media Handbook, set the security options to allow visibility to "friends only."[47] Those settings can be customized further to apply even more stringent controls over information sharing. These settings are accessed within Facebook by clicking *Account > Privacy Settings.*

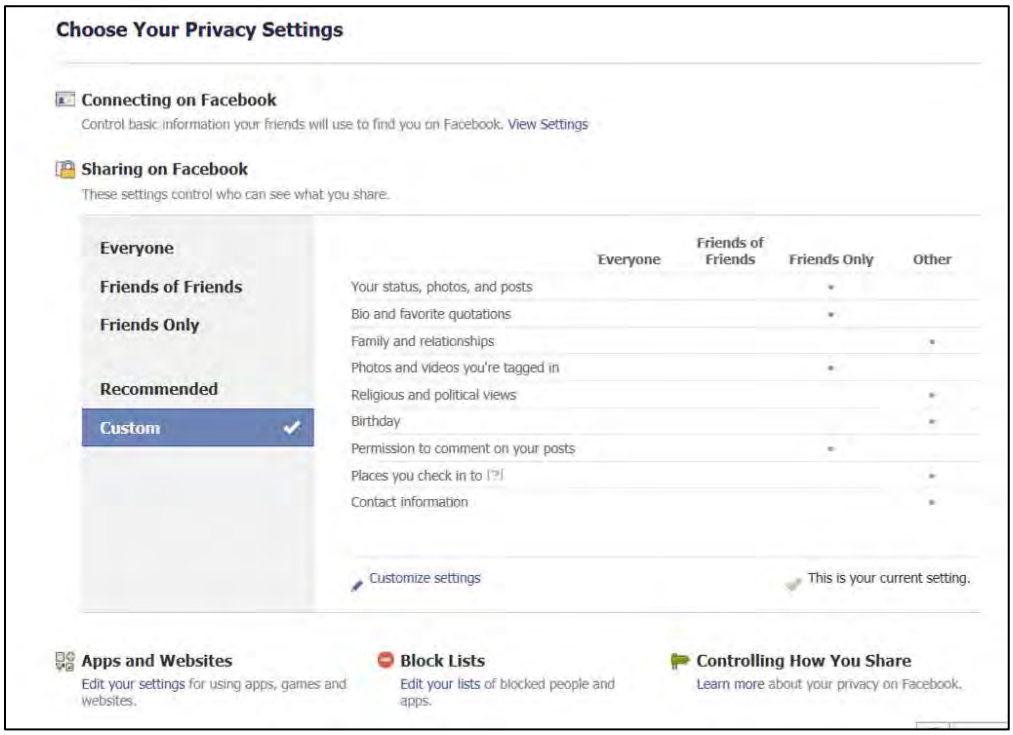

Figure 3 Facebook Privacy Settings[48]

Third rule, only share information online that can be shared with a stranger. Because social media and a user's online presence are the opposite of anonymity, viewers of a profile could include an employer, a spouse, parents, and children. Avoid the possibility of posting something that is embarrassing and harmful to personal privacy and reputation. Fourth rule, a user should carefully

---

[47] Office of the Chief of Public Affairs, 5.

[48] Facebook screencapture of privacy settings as of 18 April 2011.

choose who he links to and befriends in social media. A user must control who he allows onto his network of friends and associates. Users should avoid the trap of befriending strangers in order to give the appearance of popularity, as strangers may not have the user's best interests in mind. Therefore, it is crucial that the user control whom he allows on his network. Fifth rule, soldiers should turn off the GPS function on their phones and devices when deployed, at training or while on duty where giving away exact grid coordinates could damage Army operations. Accomplishing this rule requires a soldier to dig into the features of his device and disable the geotagging functionality. Additionally, soldiers should never upload geotagged pictures to photo sharing websites that could have operations security significance.[49]

After the individual users address privacy concerns, these users should adopt the OPSEC measures which leads to the third recommendation. The Army should publish operations security rules for social media. While OPSEC education is an annual training requirement that every soldier must complete, in its current form, the computer-based curriculum does not take into account social media at all and is incomplete. Furthermore, the training is restricted to military personnel to take on a government computer. This means that even incomplete operations security training misses a large constituency, the soldier's friends and family. What OPSEC resources are available to the friends and family of the soldier to learn? While a Google search of 'operations security for families' will find some informative resources, there is no definitive step-by-step checklist that the soldier can share with his family and friends. Positively, individual commands are producing information packets to address the need to educate family and friends (See Appendix C).[50] Yet, a critical analysis of current social media curriculum needs to incorporate several steps that extend beyond platitudes like "Be Aware" and "Be Careful." While

[49] Office of the Chief of Public Affairs, "Social Media Roundup/Geotagging Safety." *Official U.S. Army Slideshare Profile.* April 18, 2011. http://www.slideshare.net/USArmySocialMedia/social-media-roundupgeotagging-safety?from=ss_embed (accessed April 18, 2011)

[50] A Guide for Family and Friends presented by 1st Information Operations Command (Land), Vulnerability Assessment Division, OPSEC Section

using social media during deployments, the following simple steps would go a long way to maintain OPSEC. First, do not reveal exact dates of deployment or redeployment. Second, unless their specific unit information is released through some other open source in the media, do not mention the name of their camp or specific town they are working. Third, avoid mentioning any specifics about logistics routes and the conduct of combat maneuvers (remember the IDF soldier example). Specifics include detailed information about missions, capabilities, or morale of the unit. Fourth, if cooperative host nation people are vulnerable to possible retaliation, do not use their specific names and pictures in an open forum like social media. This vulnerable group includes local-born translators, local contractors, working professionals, and their families who may find themselves under an unwelcoming spotlight if information about them is revealed to the general public. Fifth, do not reveal details on military security procedures, response times, and tactics. Sixth, do not discuss equipment or the lack thereof, to include training equipment for the Army, allied forces, and host nation forces. Seventh, do not speculate about future operations. Doing so could reveal to the enemy clues about our future intentions and plans. Eighth, if posting pictures, do not post anything that could be misunderstood or used for propaganda purposes. For example, consider if the picture could be used out of context to reflect poorly on whatever was the intended purpose. Ninth, carefully evaluate every picture for details that may compromise security measures and, therefore, violate OPSEC. Tenth, never post information about casualties (friendly or enemy) or combat actions before the official release of information by the command. Lastly, do not spread or pass on rumors about information that violates OPSEC. No matter how salacious or important the information may appear on the surface, use the chain of command and official channels to verify information.

If OPSEC and careful use of social media is to become second nature then the Army needs a youth outreach program similar to BoostUp to educate digital natives about the risks of

social media.[51] While the BoostUp program targets youth at risk for not graduating from high school, the military could expand its role by advocating education and safe social media behaviors. The Army could sponsor an education program that would take place in school and in the home that would help parents and teachers manage this extraordinary transition to a globally connected society. This strategy would encourage solid social media habits and likely foster goodwill with the public.

Lastly, the Army should fund a robust social media team. In a recent interview, Major Juanita Chang noted that that her office was not funded to run social media for the Army. Nevertheless, she established an ad hoc social media team within her department.[52] Considering that so many soldiers are now using social media on a daily basis, and the potential for increased risk, it appears prudent for the Army to fund a team dedicated to engage and shape the future of social media. This social media team could provide soldiers and senior leadership dedicated support in their social media endeavors. They could allocate resources to detect emerging threats and technologies and immediately disseminate prevention steps throughout the organization through e-mail and social media. While some people will consider this information a nuisance or even spam, the commands' emphasis on safe social media practices cannot be overlooked and ignored.

The creation of a social media team should be coupled with the development of a secure website with algorithms that check a potential status update for sensitive information prior to posting. While the website cannot replace OPSEC regulations and commonsense, it could inform the judgment and reasoning of soldiers, their families, and friends before they post. Soldiers could go there for education, testing, and to double-check what they post online. Building on this idea,

---

[51] U.S. Army, "BoostUp," http://www.boostup.org/en (accessed March 20, 2011). According to the website: BoostUp is about giving potential graduates at-risk of dropping out the support they need to stay in school and on-track for graduation. This site is full of great resources and ideas to help you make a difference in the lives of students.

[52] Chang, 2010.

the Army turns the website into an application for a variety of smartphones that downloads for free. An additional feature, the Army increases the functionality of the application so that it can assist civilian companies in the workforce. The application would warn the user about posting and revealing information damaging to personal privacy or work life. Additionally, the program would evaluate and, if required, strip geo-tagging information from photos. If the military created this website correctly, it would entertain people to maintain interest and at the same time educate. The Army would position itself as a champion for safe social media discourse and foster sound social media habits by all.

Without initiatives to address social media at all levels, it appears that bureaucratic inertia of a conservative military culture will ignore the changing social media environment. The reality is social media technology will continue to evolve without the military's consent. The Army can institute training that raises awareness of these dangers for all service members. Ideally, social media becomes a manageable medium to communicate the right messages and maintain good order and discipline within the Armed Forces. Bottom line, all military personnel require training on appropriate use of social media now.

Conclusion

With the speed at which social media grows and multiplies, operations security training needs to adapt just as quickly. New and emerging technologies require evaluation against common sense operations security regulations that lay the framework by which individual user behavior is evaluated. More specifically, individual user training needs evaluation (at a minimum) of once a year for content and relevance to the changing social technology environment. Although OPSEC training is an annual training requirement, the computer-based training curriculum does not take into account many of the obvious threats and pitfalls associated with social media. Social media use across the various devices and platforms needs to be specifically

addressed either within OPSEC training or as stand-alone instruction. Culture within the military must adapt to the changing information environment.

The Army leadership needs to change and adapt to the operating environment. Anthony Bell wrote an essay on *The Myth of Generational Tensions* that highlighted some leadership insights. Bell promotes the idea that digital immigrants/Baby Boomer generation will have to adapt their leadership to the changing times and not have digital natives/Generation Y/millennial's change to older modes of thought. Leaders understand their people and their limitations; they also understand their own limitations. Therefore as a means of self-improvement, great leaders are also lifelong learners that are willing to "test and challenge their own assumptions."[53]

Leadership at all levels is the key. By educating and empowering soldiers, the Army can police itself. Given that junior members tend to be more internet savvy, and spend more time on social networks, they are perfectly positioned to recognize risks that senior leadership might overlook. Therefore, any training program must be fluid in its ability to advance with technology. This is an area in which forward-thinking leadership can enact systems and procedures to actively analyze and re-establish guidelines on a regular basis. Vigilance and rules prevented a potentially disastrous situation for the Israel Defense Force. The digital native needs awareness to be vigilant, even when 'harmlessly' using social network sites to share their lives.

Whatever methods the military decides to use requires training and vigilance to mitigate risk to allow its use to benefit Soldiers, but current methods are not sufficient. Returning social media to the list of unauthorized activities is not a useful solution either. Digital natives will continue to use social media whether it is officially sanctioned or not. Because technology is changing so rapidly, policymakers should focus on promoting positive online behaviors and not the technology. It is the Army's responsibility to educate service members as to what is

[53] Anthony Bell, "The Myths of Generational Tensions," *Leader to Leader,* 2010, 7-10.

acceptable and what is not acceptable online behavior. The Army can, and needs to, institute training that raises awareness of these dangers. A dynamic use of new media constructs should be utilized, not an unofficial document (in the form of a handbook) that lacks the weight and scope needed to combat this serious threat. In the end, the Pandora's Box of social media can become a manageable medium to communicate the proper messages and maintain order and discipline within the Armed Forces.

The DoD should have already thought of these things before issuing the policy, and maybe some of these have been answered, but those answers are not immediately evident. The individual Soldier still needs a lot of guidance on this topic. If security professionals can be guilty of letting down their guard -- as the Robin Sage Experiment so clearly illustrated – then troops require even more knowledge and ongoing training to safeguard OPSEC. With the allowance of social media, only vigilance will prevent social media from backfiring on the Army's brave soldiers.

APPENDIX A

DUE TO COPYRIGHT RESTRICTIONS,

APPENDIX A IS NOT INCLUDED

IN THIS ELECTRONIC EDITION.

The chart is available at:

http://mashable.com/2010/02/10/facebook-growth-infographic/

APPENDIX B

ESSENTIAL FUNCTIONS OF SOCIAL MEDIA COMMUNICATION

1. Remaining Timely – Social media sites and mobile technologies let civilians share information in near-real-time with potentially global audiences. DoD must be supplied with at least the same capabilities to ensure accurate information is released in a sufficient window of time.

2. Preventing and Countering Misinformation / Disinformation – Due to the speed and ubiquity of communication today, stories can quickly reach large audiences without going through the media or other filters for authentication. DoD needs its own independent voice to ensure factual information reaches the right audiences in a timely manner, and that we are able to set the record straight when necessary.

3. Ensuring an Independent Voice – With U.S. media organizations consolidating, fewer resources are available for them to cover stories. DoD was already challenged to earn mainstream media coverage in the traditional media environment; however, direct access to external audiences through social networks means DoD can mitigate some of that reduced capacity.

4. Reaching a Distributed Audience – With servicemembers, civilians and families spread across the globe, DoD needs to communicate using a variety of platforms in ways that are convenient and familiar to our audiences. This holds especially true for internal communication.

5. Empowering Servicemember Communicators – Commanders all agree that DoD's servicemembers are its best messengers. They should be supplied with the access and training needed to help them share their stories using tools they know.

6. Improving Transparency and Service – Social media tools enable direct government-to-citizen engagement and can improve customer service across a variety of functions. At the same time, by taking place in a public forum and within networks of linked people, these interactions make it possible for larger audiences to benefit from individual transactions.

7. Enabling Two-Way Dialogue – Successful communication involves speaking and listening, and social media tools allow DoD to do both efficiently and in a public forum. The information garnered through social media engagement can provide greater context for DoD actions and messages, and can help improve how DoD frames its operations and policies. This applies not just to domestic U.S. communication, but also to DoD communication overseas.

8. Monitoring Public Opinion – Because conversations are taking place in public forums, DoD can use social media to gauge public opinion on a variety of topics, even in the absence of direct engagement.

APPENDIX C

What Can You Do?

There are many countries and organizations that would like to harm Americans and degrade our influence in the world. It's possible, and not unprecedented, for spouses and family members of U.S. military personnel to be targeted for intelligence collection. This is true in the United States and especially true overseas! What can you do?

Be Alert

Foreign governments and organizations collect significant amounts of useful information by using spies. A foreign agent may use a variety of approaches to befriend someone and get sensitive information. This sensitive information can be critical to the success of a terrorist or spy, and consequently deadly to Americans.

Be Careful

There may be times when your spouse cannot talk about the specifics of his or her job. It's very important to conceal and protect certain information such as flight schedules, ship movements, temporary duty (TDY) locations, and installation activities, for example. Something as simple as a phone discussion about where your spouse is deploying, or going TDY, can be very useful to our enemies.

"OPSEC is a vital element in protecting the Army's soldiers and missions, and I want to stress how vital a role every member of the team plays in ensuring that we deny our adversaries potentially useful information.

"Whether we are on duty or off duty, we cannot afford to let our guard down. Your diligence in OPSEC is key to ensuring our effectiveness in operations and our collective safety. Together, we will succeed."

Maj. Gen. Keith B. Alexander
Commanding General
U.S. Army Intelligence and Security Command

Thank You

Thank you for taking the time to read this guide. Our goal is to provide you with a greater understanding of the Army's security concerns. The information in this guide is not intended to frighten you or make you suspicious that everyone you meet is a secret agent or terrorist. But stay alert – if a stranger shows excessive interest in the affairs of your family members, military or not, notify the authorities.

OPSEC

OPERATIONS SECURITY

A Guide For Family and Friends

Presented by

1st Information Operations Command (Land), Vulnerability Assessment Division, OPSEC Section

What Is OPSEC?

Operations Security, or OPSEC, is keeping potential adversaries from discovering our critical information. As the name suggests, it protects our operations – planned, in progress, and those completed. Success depends on secrecy and surprise, so the military can accomplish the mission faster and with less risk. Our adversaries want our information, and they don't concentrate on only soldiers to get it. They want you, the family member.

You Are A Vital Player In Our Success!

As a family member of our military community, you are a vital player in our success, and we couldn't do our job without your support. You may not know it, but you also play a crucial role in ensuring your loved one's safety. You can protect your family and friends by protecting what you know of the military's day-to-day operations. That's OPSEC.

Protecting Critical Information

Even though information may not be secret, it can be what we call "critical information." Critical information deals with specific facts about military intentions, capabilities, operations or activities. If an adversary knew this detailed information, our mission accomplishment and personnel safety could be jeopardized. It must be protected to ensure an adversary doesn't gain a significant advantage.

By being a member of the military family, you will often know some bits of critical information. Do not discuss them outside of your immediate family and especially not over the telephone.

Examples Of Critical Information

- Detailed information about the mission of assigned units.
- Details on locations and times of unit deployments.
- Personnel transactions that occur in large numbers (Example: pay information, powers of attorney, wills, deployment information).
- References to trends in unit morale or personnel problems.
- Details concerning security procedures.

Puzzle Pieces

These bits of information may seem insignificant. However, to a trained adversary, they are small pieces of a puzzle that highlight what we're doing and planning. Remember, the elements of security and surprise are vital to the accomplishment of our goals and our collective personnel protection.

- Where and how you discuss this information is just as important as with whom you discuss it. Adversary agents tasked with collecting information frequently visit some of the same stores, clubs, recreational areas, or places of worship as you do.
- Determined individuals can easily collect data from cordless and cellular phones, and even baby monitors, using inexpensive receivers available from local electronics stores.
- If anyone, especially a foreign national, persistently seeks information, notify your military sponsor immediately. He or she will notify the unit OPSEC program manager.

OPSEC IS A FAMILY AFFAIR.

All Family Members Are Part Of The Army's OPSEC Team. They Need To Protect Information To Ensure The Safety Of All Our Soldiers, Civilians, And Army Families.

DISCUSS OPSEC WITH YOUR FAMILY

Bibliography

Affairs, Office of the Chief of Public. "U.S. Army Slideshare." *Army Social Media Handbook 2011.* January 25, 2011. http://www.slideshare.net/USArmySocialMedia/army-social-media-handbook-2011 (accessed January 26, 2011).

Air Force Public Affairs Agency Emerging Technology Division. "New Media and the Air Force." *U.S. Air Force.* April 6, 2009. www.af.mil/shared/media/document/AFD-090406-036.pdf (accessed October 23, 2010).

Bell, Anthony. "The Myths of Generational Tensions." *Leader to Leader*, 2010: 7-10.

Bernays, Edward. *Propaganda.* New York: Horace Liveright Publishing, 1928.

Bokma, Lee. *Strategic Communication for Tactical Leaders.* Master's Thesis, Fort Leavenworth: Command and General Staff College, 2010.

Brown, Brittney. *The Way Ahead for DoD Social Media Policy.* February 9, 2011. http://armylive.dodlive.mil/index.php/2011/02/the-way-ahead-for-dod-social-media-policy/ (accessed February 13, 2011).

Caldwell IV, William B., Dennis M. Murphy, and Anton Menning. "Learning to Leverage New Media: The Isreali Defense Forces in Recent Conflicts." *Military Review*, 2009: 2-10.

Chang, Juanita, interview by Todd Moe. *Director of Online and Social Media Division of the Office of the Chief of Public Affairs* (September 25, 2010).

Corman, Steven R, and Jill S. Schiefelbein. "Communication and Media Strategy in the Jihadi War of Ideas." *Arizona State University.* 2006. http://www.asu.edu/clas/communication/about/terrorism/publications/jihad_comm_media.pdf (accessed December 8, 2010).

Dash, Raj. *Does Social Media Compromise Military Operations?* March 4, 2010. http://www.socialtimes.com/2010/03/does-social-media-compromise-military-operations/ (accessed March 28, 2011).

Dunlop, Laurie. *When It Comes to Social Media, the U.S. Army Says, "Have at it!" Just Remember OPSEC 101.* January 24, 2011. http://www.netstrategies.com/blog/web-content/when-it-comes-to-social-media-the-u-s-army-says-have-at-it-just-remember-opsec-101 (accessed January 24, 2011).

Evangelista, Benny. "Too much sharing online?" *San Francisco Chronicle*, December 30, 2009: DC.1.

Fabrizio, Elliott. *The Dangers of Friending Strangers: the Robin Sage Experiment.* July 21, 2010. Robin Sage Experiment. The experiment created fake Facebook, Twitter and LinkedIn profiles under the alias, "Robin Sage." A photo of a cute girl (borrowed from an adult website) and the job title "Cyber Threat Analyst" completed the fake profiles. (accessed October 21, 2010).

Facebook Inc. *Facebook.* April 18, 2011. http://www.facebook.com/?ref=logo#!/settings/?tab=privacy (accessed April 18, 2011).

—. *Facebook Press Room.* March 20, 2011. http://www.facebook.com/press/info.php?statistics (accessed March 20, 2011).

Flatley, Joseph L. *US Army Connecting Soldiers to Digital Applications program putting smartphones in soldiers' hands this February.* December 14, 2010.

http://www.engadget.com/2010/12/14/us-army-connecting-soldiers-to-digital-applications-programs-put/ (accessed March 23, 2011).

Frazier, Karen. *Social Media Privacy and the Armed Forces.* February 15, 2011. http://www.reputation.com/how_to/social-media-privacy-us-military/ (accessed February 15, 2011).

Goodchild, Joan. *10 Security Reasons to Quit Facebook (And One Reason to Stay On).* March 22, 2010. http://www.csoonline.com/article/print/584813 (accessed August 18, 2010).

—. *The Robin Sage experiment: Fake profile fools security pros.* July 8, 2010. http://www.csoonline.com/article/598906/the-robin-sage-experiment-fake-profile-fools-security-pros?page=1 (accessed October 24, 2010).

Hampton, Michael. *Army: "Soldier blogging unchanged" in new OPSEC regulation.* May 3, 2007. http://www.homelandstupidity.us/2007/05/03/army-soldier-blogging-unchanged-in-new-opsec-regulation/ (accessed March 25, 2011).

Interagency OPSEC Support Staff. *National OPSEC Program.* February 14, 2011. https://www.iad.gov/ioss/department/opsec-glossary-of-terms-10026.cfm (accessed February 14, 2011).

Mackey, Robert. *Israeli Raid Canceled After Facebook Leak.* March 3, 2010. http://thelede.blogs.nytimes.com/2010/03/03/israeli-raid-canceled-after-facebook-leak/ (accessed March 10, 2011).

Merritt, Roxie. *DoD Access to Social Media and Social Networking Sites.* Internal, Washington DC: OASD Public Affairs, 2009.

Moe, Briana, interview by Todd Moe. *Concerning Operations Security on Deployment* (February 14, 2011).

Mullen, Mike. *From the Chairman - Strategic Communication: Getting Back to Basics.* August 28, 2009. http://www.jcs.mil/newsarticle.aspx?ID=142 (accessed March 28, 2011).

Murphy, Kate. *Web Photos That Reveal Secrets, Like Where You Live.* August 11, 2010. http://www.nytimes.com/2010/08/12/technology/personaltech/12basics.html (accessed March 5th, 2011).

Myers, Jimmy. "Some worry about social networking sites: Expert: Third-party applications may put users at risk." *McClatchy - Tribune Business News*, November 30 , 2009.

Office of the Chief of Public Affairs. "Social Media Roundup/Geotagging Safety." *Official U.S. Army Slideshare Profile.* April 18, 2011. http://www.slideshare.net/USArmySocialMedia/social-media-roundupgeotagging-safety?from=ss_embed (accessed April 18, 2011).

Online and Social Media Division, Office of the Chief of Public Affairs. "US Army Social Media Handbook." *Carlisle Barracks.* January 2011. http://www.carlisle.army.mil/dime/documents/Army%20Social%20MediaHandbook_Jan2011.pdf (accessed February 15, 2011).

Palfrey, John, and Urs Gasser. *Born Digital: Understanding the First Generation of Digital Natives.* New York: Basic Books, 2008.

Paul, Ian. *It's Quit Facebook Day, Are You Leaving?* May 31, 2010. http://www.pcworld.com/article/197621/its_quit_facebook_day_are_you_leaving.html (accessed July 31, 2010).

Pierri, Vincent. *Letters from the front chronicle a World War II soldier's ordeal.* May 31, 2010. http://www.dailyherald.com/story/?id=384105 (accessed September 31, 2010).

Qualman, Erik. *Social Media Revolution Video (Refreshed).* May 5, 2010. http://www.socialnomics.net/2010/05/05/social-media-revolution-2-refresh/ (accessed October 12, 2010).

Saleem, Muhammad. *Visualizing 6 Years of Facebook [INFOGRAPHIC]*. February 10, 2010. http://mashable.com/2010/02/10/facebook-growth-infographic/ (accessed February 20, 2011).

Salta, Alex. *Conversations With Communicators: Juanita Chang, U.S. Army.* March 11, 2011. http://ohmygov.com/blogs/general_news/archive/2011/03/11/conversations-with-communicators-juanita-chang-u-s-army.aspx (accessed March 24, 2011).

Shira, Rubin. *Soldier's Facebook leak forces Israel to cancel raid.* March 3, 2010. http://seattletimes.nwsource.com/html/nationworld/2011249564_isfacebook04.html (accessed March 11, 2011).

Soto, Lucy. "Not-so-private Web: Information leaks on social networks can leave users vulnerable." *The Atlanta Journal - Constitution*, February 14, 2010: p. B.1.

U.S. Army. *BoostUp.* 2011. http://www.boostup.org/en (accessed March 20, 2011).

U.S. Army Public Affairs. "U.S. Army Social Media Handbook 2011." *United States Army Slideshare.* February 12, 2011. http://www.slideshare.net/USArmySocialMedia/army-social-media-handbook-2011 (accessed February 25, 2011).

U.S. Forces - Afghanistan Public Affairs. *U.S. Forces - Afghanistan Announces Social Networking Initiative.* June 2, 2009. http://www.bagram.afcent.af.mil/news/story.asp?id=123152545 (accessed February 12, 2011).

U.S. JFCOM Joint Warfighting Center. *Commander's Handbook for Strategic Communication and Communication Strategy.* Suffolk: USJFCOM Joint Warfighting Center, 2009.