REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
06/04/2017	Master's Thesis	SEP16-APR17

4. TITLE AND SUBTITLE

Connected? – Examining the threats posed to SOF personnel and their families through social media exploitation and the existing policies in place to mitigate them.

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)

Hora, James H., LCDR, USN

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

United States Marine Corps
Command and Staff College
Marine Corps University
Quantico, Virginia 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER

N/A

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

Dr. Lauren Mackenzie

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

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Members of the United States military, particularly Special Operations Forces (SOF) members are challenged with balancing the growing use of social media with their concern for privacy and security as modern communication and technologies evolve. As technology advances, personal electronics like laptops, smartphones, and now wearable devices have accelerated the ease and frequency at which people interact in an expanding digital world. The mass volume of personal information being generated coupled with readily available public, private, and government collected data poses a growing vulnerability to the privacy and security of SOF personnel and their families. The aggregation of mass data enables nefarious actors (petty or organized criminals, state or non-state actors, or terrorists) the information necessary to perpetrate identity theft, or to harass or target individuals or groups. The heightened visibility and media exposure highlighting the operational successes of the SOF community over the past fifteen years, has increased concerns that too much information is being generated that can be used to target the SOF community or individual service members. This research paper will examine the potential hazards and exploitation vulnerabilities to SOF member's unsafe usage of social media.

15. SUBJECT TERMS

Special Operation Forces, SOF, Family, Social Media, Vulnerabilities, Threat, Identity Theft, Targeting, Exploitation,

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			USMC Command and Staff College
Unclass	Unclass	Unclass	UU	52	**19b. TELEPHONE NUMBER** *(include area code)* (703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

TITLE:
Connected? – Examining the threats posed to SOF personnel and their families through social media exploitation and the existing policies in place to mitigate them.

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR:

LCDR J. H. Hora

AY 16-17

Mentor and Oral Defense Committee Member: ___ Dr. Lauren Mackenzie_____
Approved: _____
Date: 27 Mar 17

Oral Defense Committee Member: ____Professor Michael Lewis_____
Approved: _____
Date: 27 Mar 2017

EXECUTIVE SUMMARY

Title: Connected? – Examining the threats posed to SOF personnel and their families through social media exploitation and the existing policies in place to mitigate them.

Author: Lieutenant Commander James H. Hora, United States Navy

Thesis: This research paper will examine vulnerabilities to SOF personnel and their families through the exploitation of social media and mass data; assess the various kinds of threats posed by social media; and *make recommendations* regarding existing DoD and SOCOM policies to mitigate the unforeseen consequences associated with social media exploitation.

Discussion: Members of the United States military, particularly Special Operations Forces (SOF) members are challenged with balancing the growing use of social media with their concern for privacy and security as modern communication and technologies evolve. As technology advances, personal electronics like laptops, smartphones, and now wearable devices have accelerated the ease and frequency at which people interact in an expanding digital world. The mass volume of personal information being generated coupled with readily available public, private, and government collected data poses a growing vulnerability to the privacy and security of SOF personnel and their families. The aggregation of mass data enables nefarious actors (petty or organized criminals, state or non-state actors, or terrorists) the information necessary to perpetrate identity theft, or to harass or target individuals or groups. The heightened visibility and media exposure highlighting the operational successes of the SOF community over the past fifteen years, has increased concerns that too much information is being generated that can be used to target the SOF community or individual service members. This research paper will examine the potential hazards and exploitation vulnerabilities to SOF member's unsafe usage of social media, and proposes changes to SOF policies in orders to increase service member awareness and mitigate those vulnerabilities.

Conclusion: The SOF community needs to understand that the vulnerabilities of social media usage is not exclusively an Operational Security (OPSEC) concern; it can have immediate and lasting impacts to an individual SOF member's ability to maintain service eligibility and high performance standards. SOF leadership must adopt a proactive approach (with dedicated resources focused specifically towards SOF family awareness) in advancing awareness and implications of unguarded social media participation and advocating the education for service members and their families in order to limit vulnerabilities associated with careless social media usage. With expanded awareness and vigilance, the SOF community can mitigate disruptions to operational requirements.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE

VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

TABLE OF CONTENTS

Page

PREFACE

Ten days after placing an online advertisement for a used car I was selling, I received an email inquiry from an interested out-of-state buyer, asking for further information. We went back and forth over several emails as I tried to answer his questions about the cars condition and maintenance history. It became apparent early on that he was very interested in buying the car. There was nothing out of the ordinary, until he sent me an email asking if I lived at the address he included in the email, stating "Googles a great research tool." I was taken off guard, because it was my address, and when I placed the ad, I had only provided the city and state for where the car was located. After a general Google name search on myself, I was able to find my address and other information that I did not know could be so easy to find. Moreover, I was surprised to learn and see that Google's street view on Google Map had captured an image of the car I was selling in front of my house, confirming my address in the buyer's search.

Although the buyer turned out to be legitimate and I sold the car without issue, it proved to be an unnerving experience, because my wife and I are not social media (i.e. Facebook or Twitter) users and we try to limit our digital exposure. The whole experience increased my interest in the new social media culture. Moreover, I was shocked to realize just how much information, accurate and detailed information, was aggregated and available about our lives for others to see and potentially exploit. Having been in the SOF community for over two decades, I grew up in the old guard or "Quiet Professional" generation, where sharing work information, experiences, and photos with family or friends rarely occurred face-to-face, let alone posted to the internet for public consumption. I now find myself, balancing my increased concern for family privacy and security with my daughter's blind obsession with social media and her desire for uninterrupted connectivity in the here and now generation. The mass volume of personal

information being generated coupled with readily available public, private, and government collected data poses a growing vulnerability to the privacy and security of our SOF personnel and their families. This increased use and dependence on social media spurred my curiosity, fueling the research for this paper.

A wide range of sources were collected and reviewed during the development of this research paper. The literature review focused on resources available through the United States Marine Corps University (USMCU) Gray Research Center (GRC) library and databases, the Defense Technical Information Center (DTIC) archives, and the internet to identify books, articles, blogs, videos, journal entries, and Department of Defense (DoD) social media policies, instructions, and regulations. Additionally, the USSOCOM Identity Management (IdM) office was contacted in search of social media policies and training aids to frame the scope of the topic and to assess the current efforts to mitigate SOF social media usage concerns. This research paper will examine the potential hazards and exploitation vulnerabilities to SOF member's unsafe usage of social media, and proposes changes to SOF policies in orders to increase service member awareness and mitigate those vulnerabilities.

ACKNOWLEDGEMENT

First and foremost, I would like to thank my wife and daughter for their unwavering support during this academic year. Their selfless commitment and support over the last nine months permitted me the opportunity to grow personally and professionally in the achievement of my academic goals.

I would like to thank my Masters of Military Studies mentor, Professor Mackenzie for her vision, patience, and mentorship. Your wisdom and guidance were invaluable in shaping and completing this research paper.

I would also like to thank Mr. Desmond, Identity Management Chief, at SOCOM for supporting this paper with your time, material expertise, and by providing valuable research material to better understand and frame the growing concerns of SOF social media usage.

I would like to extend my sincere gratitude to Dr. Di Desidero, Ms. Hamlen, and Ms. Wells, Director and Instructors, at the Marine Corps University Leadership Communication Skills Center. Your writing guidance and saint like patience during this academic year were invaluable in shaping my academic success.

Lastly, I would like to extend a special thanks to my civilian and military faculty advisors, Professor Lewis and Lieutenant Colonel Curtright, your unwavering support and encouragement throughout this academic school year were greatly appreciated.

Connected?

Examining the threats posed to SOF personnel and their families through social media exploitation and the existing policies to mitigate them

The problem is not the technology, but the way we think about the technology.[1]

- *Jaron Lanier, computer scientist*

INTRODUCTION

The evolution of modern communication technologies and interactive social media platforms continues to invite participation from an ever-increasing audience. Social media, as defined by the US Chief Information Officer (CIO) and the Federal CIO Council is "the future of communication, a countless array of internet based tools and platforms that increase and enhance the sharing of information. This new form of media makes the transfer of text, photos, audio, video, and information in general increasingly fluid among internet users."[2] In other words, social media users create virtual communities and networks to share personal messages, ideas, interests, and feelings. The convenience, main stream usage, and reliability of social media platforms, permits people to stay connected to anyone in near real-time from virtually anywhere around the world. The ability to interact on these platforms allows the free flow of information with minimal or no delay, where social media platforms like Facebook and Twitter among many others have been accepted as a primary means of communication. Convenience aside, the sheer volume of personal information being broadcasted through these social media networks, coupled with the mass data collected through aggregated public, private, and or government datamining efforts, represents a notable vulnerability to the privacy and security of all users.

Although most of the information propagated on social media sites can be viewed as just benign social interaction between family and friends, personal and private information is often too willingly offered up under the naive impression that the conversations are only viewable or received by the intended audience. Interacting on social media has becoming increasingly personal, creating an ego or "me" factor encompassing social media.[3] Unfortunately, this can create the illusion that users alone are at the center of social media conversation with everyone

and everything revolving around the user.[4] If individuals feel they are at the center of their social media experience, they may not recognize the significance and breadth of the personal information they share with others in the digital world. Are social media users more willing to share personal information through digital mean than they might not do face-to-face? Social media sites, data aggregators, the government, and nefarious actors are banking on it.

Why does this matter? How does this present a vulnerability to the military, particularly Special Operation Forces (SOF) personnel and their families? Does this create an opportunity for nefarious actors to take advantage of mass information to target SOF specifically? Gabriel Weimann asserts that:

> Many soldiers unwittingly post detailed information about themselves, their careers, family members, date of birth, present locations, and photos of colleagues and weaponry. Even if the information does not give details about the logistics of troop movement, it could potentially endanger the friends and relatives of military and security personnel.[5]

Weimann's statement highlights the potential targeting dangers posed by exposing too much personal information, which nefarious actors can use to harass military personnel or to perpetrate criminal activity like identity theft - all of which would have an impact to a service member's ability to do their job.

Members of the US Military are a prime target for identity theft. Service members have a regular paycheck and most relocate every two to three years, both of which are attractive to a would-be thief due to the fact that money comes in twice a month and they might get away with identity theft longer without notice because the service member has a pattern of moving.[6] Active duty service members and retired veterans are twice as likely to file identity theft complaints as a percentage than that of their civilian counterparts.[7] For a SOF member, if the stress and financial losses attributed to identity theft were not enough, it can impact the member's ability to obtain

and maintain a security clearance. All SOF operators have a minimum of a SECRET security clearance, but a TOP SECRET security clearance is required for operators accessing more sensitive information needed to plan and execute more sensitive missions. Identity theft can result in a bad credit report, preventing a SOF member's ability to hold a security clearance, and without a clearance, a SOF member cannot access information required in the performance of their primary duty.

Finally, over the past fifteen years of sustained combat operations, coupled with the publicized recognition of highly successful SOF operations, the value of targeting SOF (the community or the individual) by extremists has increased. Although, no specific or credible information of terrorists actively targeting SOF were identified in the research for this paper, they have the potential to become high value targets to extremists. Moreover, the high volume of SOF books published in recent years to include endless news media appearances and political grandstanding has sharply increased SOF public persona. As long as the publicized tales of successful SOF operations are told, the threats to SOF will continue to extend from the battlefield back to their state side parent commands and to their families.

In recent years, the US Military has adopted and increasingly incorporated social media as an efficient tool for disseminating relevant information to service members and their families. Likewise, service members have increased their use of social media to both network with others and attend to personal affairs - in all cases, the military and the service member can wittingly or unwittingly expose day-to-day pattern of activity or disseminate Personally Identifiable Information (PII) vulnerable to exploitation. The combination of military details and personal information presents an unnervingly accurate and targetable opportunity for potential nefarious actors. As with the greater civilian population, the distractions that come with social media

"hyper connectivity" poses a threat to our service members' ability to focus on their primary job - defending the American way of life. This can be more disruptive to our front-line troops and especially to SOF supporting high operation tempo overseas deployments.

This research paper will examine the impacts of social media usage in an effort to: 1) Identify vulnerabilities, threats, and impacts to the SOF users, 2) Differentiate between personal impacts and Operational Security (OPSEC), 3) Highlight the applicability of the Communication Privacy Theory to understand the disconnect between individuals' expectations surrounding social media use and the reality of its implications, 4) Assess Department of Defense (DoD) and United States Special Operations Command (USSOCOM) policies, regulations, and guidance for service member social media usage, and, finally, 5) Make recommendations to mitigate negative impacts of social media usage.

UNDERSTANDING THE PROBLEM

The future of communication is being charted by the current use, convenience, and rapidly growing dependence on social media in the digital world, with no shortage of advocates and cynics openly providing their opinions or research on the topic. Jason Lanier, computer scientist and co-creator of start-up companies acquired by Oracle, Adobe, and Google, and author of *Who Owns the Future*, views the evolution of communication through modern technology from a monetary perspective. Lanier sees vast potential in the digital world as a wealth generating utopia through the expansion of one's productivity, creativity, and intellect. But he recognizes that the digital world is a flawed utopia, noting that power and money controlled by the few "keep the new ledgers, the giant computing services that model you, spy on you, and predict your actions, [and] turn your life activities into the greatest fortunes in history."[8] Information collected in the digital world has created great wealth for a few, but should

compensate all that contribute, not just the aggregators, institutions, or criminals. The internet and use of social media has transformed the way we communicate, the way we interact, and the way learn, but the digital world also presents vulnerabilities depending on the motivations and ends to which that information is used. The following sources below were reviewed in shaping a comprehensive understanding of social media benefits and potential vulnerabilities.

The Communication Privacy Management (CPM) Theory will be introduced as a means of illustrating the connection between our expectations surrounding privacy and the realities of social media usage. Its creator, Sandra Petronio suggests that "sharing confidential information always reduces privacy", while making a compelling case that there is still an expectation of privacy even when we share personal information in the process of establishing or strengthening close relationships.[9] This paper will suggest the applicability of CPM to illustrate the differences in privacy expectations when sharing information face-to-face and in the digital world.

In his 2015 book, *Terrorism in Cyberspace: The Next Generation*, Wiemann describes the growing use of the internet and social media by extremists to spread ideological propaganda, to radicalize and recruit, and for reconnaissance to target locations and people. He states that with the information available on the internet, "Terrorists can use social networking sites such as Facebook to monitor military personnel."[10] Moreover, he highlights that the US Military has increased its efforts to educate troops on the potential hazards of posting too much information about oneself or their units online. As technology continues to evolve, becomes cheaper and easier to use, we become less and less vigilant about our behavior due to its omnipresence, with which nefarious actors can gain increased access to information that can be exploited to perpetuate their agendas.

Privacy advocate, Lori Andrews, in her 2012 book, *I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy*, asserts "Social networks have become ubiquitous, necessary, and addictive. Social networking is no longer just a pastime; it's a way of life. People expect to be able to log on to Facebook or MySpace wherever they go and to tweet their every thought."[11] She describes the internet as a spider web, connecting an ever-growing number of social media platforms where users interact and leave bits of data. All the data introduces to this web becomes entangled by servers and computer programs designed to capture and consolidate information, which is ultimately available to the government and aggressive date aggregators. Andrews highlights the impacts Facebook, Twitter, Google, YouTube, and other social media services have had in eroding our personal privacy through the endless collection of information. Her assessment is that once information is out there, it is very difficult, if not nearly impossible to track or remove it without the information being repopulated by another undeleted data server.

Jacob Silverman, Author of *Terms of Service: Social Media and the Price of constant Connection*, describes the evolution of communication, societies adaptation to rapidly evolving technologies, and the growing use of social media as the predominate form of modern day interaction. People are becoming more isolated and separated from traditional societal interaction as they withdraw into the "intoxicating glow" of their impersonal smart devices and absorbed into the digital world. People regulate their interaction with others and filter the information they receive, providing them the illusion of privacy and control.[12] However, the social pressures for mass conformity persuade people to interact and openly share in the digital world in ways they would not otherwise do face-to-face. The mass production and accessibility of personal information enabled by modern technology has commoditizes all who participate.

The aggregation of user information, no matter how small and insignificant the pieces, over time, paints a detailed picture of the person as a whole.

During the source review for this paper, no DoD Policies or Instructions were identified that significantly limit or prohibit DoD employee access to Internet-based Capabilities (IbC) on the DoD Non-Classified Internet Protocol Router Network (NIPRNET). DoD Directive-Type Memorandum (DTM) 09-026 – *Responsible and Effective use of Internet-Based Capabilities,* defines IbC as "…[a] collaborative tools such as SNS [Social Networking Services], social media, user-generated content, social software, e-mail, instant messaging, and discussion forums (e.g., YouTube, Facebook, MySpace, Twitter, Google Apps).[13] Per DoD Instruction 8550.01, *DoD Internet Services and Internet Capabilities,* DoD Components Commanders will only limit DoD employee access to IbC on NIPRNET as required to safeguard operational capabilities, preserve bandwidth, and or preserve Operational Security (OPSEC).[14] The use of social media by the military has evolved into an indispensable operational planning and coordination tool, as well as a Morale, Welfare, and Recreation (MWR) tool for the individual service member to communicate with family, friends and teammates. DoD acknowledges the concerns of intentional and or inadvertent release of PII, choosing the address the issue with annual mandatory OPSEC training, but has stopped short of implementing any significant limitation to accessing to social media sites to preserve service members first amendment rights.

None of the resources reviewed for this research paper addressed the direct vulnerabilities of SOF social media usage directly, however, each resource provided a unique perspective in order to frame the utility and convenience of social media with the potential hazards of unguarded internet "hyper-connectivity". Heightened concerns over the increased use of social media in recent years has driven the SOF community to focus more resources and attention in

educating SOF members to the potential vulnerabilities of uninformed and unguarded social media use. It is therefore the authors opinion that the families currently represent the greatest social media vulnerability within the SOF community because of USSOCOMs lack of direct control or influence over civilian non-SOF members to manage or ensure awareness of the pitfalls of potentially exposing too much information. The intent of this research paper is to consolidate and extract relevant social media source material, educate users, and provide a pathway to mitigate vulnerabilities for SOF personnel.

THE SOCIAL MEDIA EVOLUTION

Every detail of your life – what you buy, where you go, whom you love – is being extracted from the internet, bundled and traded by data-mining companies.[15]

-Joel Stein, Columnist

In the modern age of rapidly advancing communication technologies and expanding use of digital media, people are faced with the predicament of balancing the convenience and ease of digital interaction with the concerns for personal privacy. Susan Barnes, debated "the uproar over privacy issues in social networks by describing a privacy paradox; private versus public space; and, social networking privacy issues."[16] in her 2006 article titled *A Privacy Paradox: Social Networking in the United States*. The intent of her argument was to highlight the concerns over how freely teenagers were divulging personal information on social networks and that society was (and still is) ill prepared to handle the potential abuses of mass data. Ten years later those teenagers arguably represent the first generation to grow up in the modern information age, where the free flow and common access to information appears to have no limit. James Beniger, proposed that:

> The rise of the Information Society itself, more than even the parallel development of formal information theory, has exposed the centrality of

> information processing, communication, and control of all aspects of human society and social behavior.[17]

As society evolves and populations grow, the collection and processing of information is required to manage, engineer, and control the populous. Information need only be consolidated and analyzed to determine how to shape and or manipulate society towards a desired end state.

Personal information populated and accessible in the digital world comes from a variety of sources; ecommerce, social media, public record, and private or government data-mining. Ecommerce information is the financial and transactional data of one's banking and purchasing patterns. Information is collected when a credit, debit, and or rewards card is used to facilitate a transaction.[18] Transactional data can consist of dates, times, locations, amount paid, and items purchased, moreover, it connects the purchaser to a specific financial institution when not paying cash. Each piece of information collected by data-mining companies (aggregators) like EXelate, RapLeaf, and Inellidyn, is worth about two fifths of a cent when sold to companies eager to learn consumer spending habits.[19] Companies use purchase history information to refine their marketing strategies and to target the interests of potential customers. It becomes apparent when your interests are being observed, when you see small advertisements from one internet site to another, relating to product you recently searched for online.

Social media information is derived from the use of computer mediated technologies where users interact and socialize in virtual communities and on networks where users create and share information, ideas, and interests. Information generated by individuals through social media is the fastest growing sector of information populating the digital world and is predicted to exceed seventy percent of all data created by 2020.[20] Personal information propagated through social media is arguably the most revealing of one's inner self and more vulnerable due to the

personal nature of the information as compared to that of ecommerce or public record information. If a SOF member has a sensitive conversation with teammates in a crowded bar, is that conversation private when others within ear shot can listen in on the details? In the case of having a conversation on social media, the volume of the conversation is irrelevant, the concern lies in what and where the user posts online.[21] Depending on user social media security settings, people may still see your posts, your digital conversations, even if they are not in your circle of friends or if a friend forwards the conversation with or without knowledge of the originator. Unintended exposure of personal information can be extremely embarrassing, jeopardizing a relationship or a SOF career. Once information is revealed on social media, it is out there, and it is nearly impossible to determine the extent to which it will be viewed, shared, or exploited.

Public record information is generated and stored by the state, county, or city when requesting and or granted a title, license, or permit. It becomes part of the public record when one purchases and titles a home; obtains a public phone number; registers a vehicle, boat, or plane; obtains a birth or marriage certificates; or receives a concealed weapons permit. The public record also stores traffic, criminal, and court records. Typically, public records are accessed by government agencies, but private business can also access these records. People finder sites like PeekYou, PeopleFinder, Intelius, Truthfinder, and Spokeo aggregate information from millions of sites across the internet including information accessed from public records, where they make it available to anyone willing to pay a nominal fee.[22] David Lazarus, describes how Harrison Tang, Spokeo founder, opted out of having his own personal information aggregated by his own company based on privacy concerns, but that "Paying customers can get people's full address, including street number, and more detailed information about who others are and what kind of life they lead."[23] Unfortunately, there are limited to no options for the

general public to opt out of these data mining efforts. The amount of information being aggregated on an individual and personal level is without precedent in human history. Some of this information will be used to better the user experience, connectivity, and convenience, but there are those that might use the information to identify, exploit, or target the SOF community or member.

CHARTING AND PROFILING THE DIGITAL WORLD

As technology expands and digital usage increases, companies will try to better understand and advance their consumer base by capitalizing on the interaction between people in the digital world. Robert Scoble and Darren Barefoot, digital strategists and marketers introduced the Social Media Starfish in 2008 (Fig. 1), mapping the social interaction landscape. Brian Solis, a digital analyst and futurist, expanded upon the Starfish idea since then, creating the current 2016 Conversation Prism (Fig. 2). The Prism provides a visual representation of the growing interaction of the individual (depicted as You at the center) with social networking sites. The prism represents numerous social media companies (players) within the interconnected sphere, all competing for the user's attention, time, input, and consumption. Each interest group of players radiating from the center, offers a different point of interest to a potential user, like, social networking, photo sharing, location services, music and video streaming, business, and ecommerce. The more the user interacts with one or more of the players, the more information is available for companies to analysis, strategize, and target client interests. Moreover, the players represented in the sphere, interact and collaborate with each other, sharing bits and pieces of information with each other to improve user interests in their platforms. Changes in the social media landscape over the last eight years are notable and reflects a dramatic increase in the

number of players that are competing for user interests as well as collecting, storing, and selling user personal information.

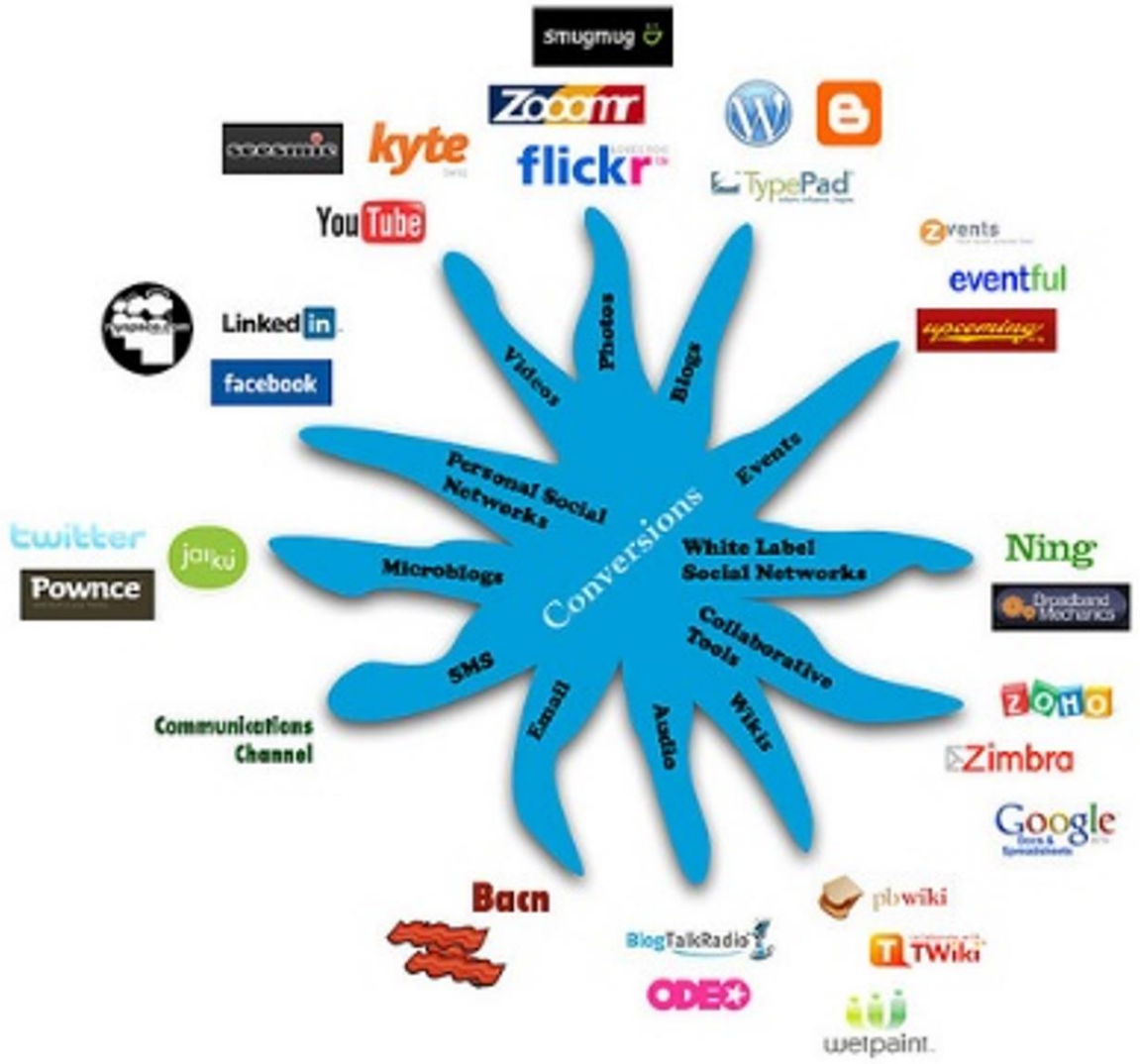

Figure 1 - The Social Media Starfish – 2008

Figure 2 - The Conversation Prism -2016

In today's fast paced ecomomy, mapping the digital consumer has become big business. Companies are willing to invest heavily for information, advancing their marketing strategies to better target a specific consumer audiance. Advertising its efforts to "Know Your Audience", GlobalWebIndex (GWI) conducts the largest ongoing digital consumer and social media

behavioral study in the world. GWI interviews and tracks over 200,000 active study participants annually and has access to a panel of ten million active internet users from thirty-three global markets, representing nearly ninety percent of the world internet audiance.[24] The study focuses on nine key areas of interest to collect, analysis, and predict holistic social media usage:

1. Demographics - The building blocks for audience creation. Combine deep demographic attributes with any of the questions in other categories to understand your target group in incredible detail.
2. Attitudes and Lifestyle - Understand the lives and lifestyles of digital consumers, from their self-perceptions and interests to their professional lives, wealth profiles and engagement with areas such as sport, travel and the web.
3. Device Ownership and Access - A detailed view on connectivity and device adoption. Understand usage of operating systems, virtual private networks and emerging devices such as smartwatches.
4. Online Activities and Behaviors - Get a cross-device view on what people are doing online, as well as the top global and local websites that they are visiting.
5. Media Consumption - Get the latest insights across on-demand content, second-screening, time spent on media and usage of connected devices such as games consoles.
6. Social Media - Understand how and why people are using social media, with deep-dives into actions specific to the top global services.
7. Apps - Quantify and trend usage across both named applications and application categories.
8. Commerce - Measure past transactions, path to purchase and intent levels across a wide range of product types & categories.
9. Marketing Touchpoints - Quantify effective marketing touchpoints for your target audiences, and understand brand discovery journeys.[25]

GWI cross-references aggregated internet data with information provided by their active social media study participants to provide companies advanced marketing strategies and profiling data for targeted audiances based on demographics, locations, interests, and associations. For SOF,

the aggregation of associations, like, family, friends, teammates, and the community are the most disconcerting, because this can link SOF members together even if they do not actively use social media. Companies like Google, Yahoo, LinkedIn, Microsoft, Expedia, and Twitter are among some 1200 companies using GWI customer profiling data.[26] The aggregation of user data has led to the commoditization of the individual. Public and private information is collected, analyzed, and exploited for corporate and potential nefarious gain, with the individual user unable to opt out of the new mass data-mining norm. So, what is in it for the individual – a better digital experience, improved convenience, or just self-aggrandizement? Does the individual truly have any control? The paper will now turn toward a discussion of the management and unrealistic expectations associated with communication privacy.

COMMUNICATION PRIVACY MANAGEMENT THEORY

In an age of digital media, do we really have any privacy?[27]
-Susan B. Barnes, Prof of Communications

Even with documented and growing privacy concerns associated with social media usage, "hyper-connected" social media enthusiasts still believe their information is private, or simply underestimate the potential significance of its dissemination. Sandra Petronio, introduced the *Communication Privacy Management Theory* (CPM), hypothesizing that people inherently do have an expectation of privacy when they are communicating private information to others. CPM offers that individuals establish *privacy boundaries* with who and how private information is shared.[28] Expanding upon the *social penetration theory*, introduced by Theorists Altman and Taylor, Petronio agrees that the disclosure of personal information is a critical element in developing close relationships with others, but she asserts that there is still an expectation of privacy that requires the consideration of her five core principles:

1. People believe they own and have a right to control their private information.

2. People control their private information through the use of personal privacy rules.

3. When others are told or given access to a person's private information, they become co-owners of that information.
4. Co-owners of private information need to negotiate mutually agreeable privacy rules about telling others.
5. When co-owners of private information don't effectively negotiate and follow mutually held privacy rules, boundary turbulence is the likely result.[29]

The theory suggests that people determine what information they share with others and that they establish negotiated boundaries on how that information is to be handled when shared. The expectation is that those entrusted with private or personal information will care for it as a co-owner, the same way the originator does. Although the theory is better suited for face-to-face communication than digital communication mainly because the negotiated boundaries are never established in social media - such "imagined" boundaries and the asymmetry between perception and reality is what this theory seeks to illustrate. Recent studies using CPM in close relationships have emphasized the importance of *motivation* as a key factor for determining how much information is revealed to a partner.[30] These findings can certainly extend to social media users in that an improved understanding of motivations by users to reveal person information (as well as increased knowledge about the motivations of those attempting to benefit from it) could potentially reduce unintended consequences.

When an individual provides personal information on social media, the information is digitized and processed through servers and computer programs, as described earlier, that are specifically designed to gather information in the process of forwarding it to the intended recipient. Social media does not discern private information from general information unless the information is encrypted before sending. This is where privacy expectation and reality diverge,

because the internet was designed to capture and share information without regard to privacy. As long as companies seek to commoditize and exploit the personal and public information of individuals, true personal privacy cannot exist on social media sites. True privacy can only exist within close face-to-face relationships amongst family, friends, and teammates or within oneself.

IS THERE SUCH A THING AS PRIVACY IN SOCIAL MEDIA?

If you are getting something for free – you and your information are the product![31]
-Dennis Desmond, USSOCOM, Identity Management Branch Chief

Shared experiences are forms of social currency. People share things to show their friends that they're investing in the conversation. Shared experiences can be shaped and steered.[32]
- Brian Solis, Digital Analyst and Futurist

The evolution and use of social media has transformed the way in which society interacts and how we are informed. The primary means of yester-year communication, Newspapers, radio, and television have given way to the internet through the use of computers, tablets, and smartphones. Between 2000-2010, newspaper sales decreased by nearly 50 percent, while news searched through social media sites increased from 33 percent to 66 percent.[33] Search engine sites, the biggest of which is Google (projected to conduct over two trillion searches annually by 2016)[34], have increased the speed and convenience of locating and presenting aggregated and searched information. How does a search on Google provide more information than you could ever want to know about the history, locations, and nearly all past operations of specific SOF units? To support the mass volume of information users demand, Google is always on, constantly searching, collecting, and listening to the mass flow of information on the internet to link information together. Google has engineered an environment where they rack-n-stack the order in which users see information. Complex algorithms analyze internet user history, patterns, and preferences to predict future interests, allowing Google and their partners to shape

user experiences and target product advertisements. How does Google make money when their service is free to the user? According to the US Securities and Exchange Commission, Google's annual profits have doubled from thirty-eight billion in 2011 to seventy-five billion in 2015.[35] Google as with other social media sites, sells user information so partner companies can target their advertising efforts. Moreover, Google has gone a step further when they launched Google Now, a product that consolidates user social media data with personal contacts, calendars, GPS locations, and interests to recommend daily activities. Jacob Silverman suggests that:

> Google Now demonstrates the extent to which the environment that social-media companies are building and herding us into are fundamentally manipulative. Armed with data that we provide (sometimes unwillingly or unknowingly), Google and its competitors are engaging in nothing less than social engineering on a broad scale, pushing us to share and share under the pretense of improving our lives and building global community when, in fact, they want nothing more than to target us with ads that they deem "relevant" and urge us to buy products from their partners. Whether they actually believe their grand prophecies only matters insofar as it provides cover for their assaults on user privacy, identity, self-expression, and autonomy. Under the paternalistic hands of Google and Facebook, we have been building digital lives only to give them away wholesale, all because the services were convenient and free and we told ourselves that we didn't know better.[36]

Social media sites provide their services to users for free, while making mass profits commoditizing their identities. In a never-ending effort to exploit the potential of evolving technology, Google has recently introduced its latest venture, the Google Home, which is advertised as a wireless speaker system commanded by the user's voice to answer question, play music, or connect to other smart devices. Basically, it is a voice activated Google search tool with an active microphone connected directly to the internet. The concept of asking a question aloud at home and receiving an immediate answer is an amazing concept and extremely convenient, but definitely raises the creepiness factor over concerns that the internet might be able to listen in on every conversation within proximity of the device. Modern technologies and

social media innovative marketing of mainstream and niche items are pushing the boundaries between convenience and privacy intrusion.

For most people, when they think of social media, the first thing that typically comes to mind is Facebook. Facebook was founded in 2004 by Harvard University drop out, Mark Zuckerberg, who over the past twelve years has grown the company to over 15,000 employees, creating a new web based social and cultural phenomenon now used by 1.18 billion active daily users.[37] Like Google, Facebook makes money by selling user information to business partners targeting the advertisement audience, generating $17.93 billion in revenue for 2015.[38] *Forbes magazine* now ranks Zuckerberg as the sixth richest person in the world with a net worth of $44.6 billion.[39] The companies stated mission "… is to give people the power to share and make the world more open and connected. People use Facebook to stay connected with friends and family, to discover what's going on in the world, and to share and express what matters to them."[40] Facebook provides a platform for users to connect and share with other selected individuals or the world as a whole depending on the user's preferences and security settings. But, regardless of your security settings, Facebook, by default, makes its account holders personal data: users' names, profile photos, lists of friends, gender, and geographic location searchable through search engines (like Google), applications, and other web sites.[41] Even if a Facebook account user never connects to a specific search engine or web site, their information might be accessible through them without the user's knowledge.

Facebooks data collection reach extends beyond Facebook account holders. Since its founding, Facebook has acquired sixty-eight companies, increasing the number of its players in different interest groups within the social media Conversation Prism, most notably WhatsApp, Instagram, and the pending purchase of LinkedIn.[42] All the companies within the Facebook

enterprise share information, where it is aggregated, creating a broader understanding of the commodity (you the product). Facebook just recently suspended its WhatsApp data sharing in the United Kingdom based on privacy advocates efforts to prevent the practice, but Facebook data sharing is still active in America.[43] Facebook, as well most other social media sites, count on their users not taking the time to read the user agreements, allowing access to their sites. Who actually reads the user agreements and terms of usage for all or any of the applications or services they use?

Most users freely select "OK" or "Agree" when prompted to verify and accept new application features or notified of changes to user agreements without reading or understanding what they are signing up for. Joan Goodchild asserts that:

> Many privacy advocates feel Facebook needs to do a better job of educating folks about what the new feature is, what it does, and how to opt in or out. Many also feel a user should always be opted out of new features automatically, and should then have to opt in themselves. But it is often the other way around when Facebook rolls out these features.[44]

Social media sites update their usage agreement and terms every time the site is upgraded or when a new feature or connection is added, but users have become numb to the frequency they receive these requests and do not take the time to read them.

Social media sites like Facebook roll out new features vailed as enhancements, improving the user experience, or increased conveniences where users are automatically enrolled into the new features without any opportunity to opt-out. For instance, in August 2010, Facebook acquired Divvyshot, a photo-sharing website with proprietary software capable of tagging photos, linking them to specific events.[45] By June 2011, Facebook had automatically enrolled all Facebook users into its new tagging feature (without prior notification or consent), using facial

recognition technologies to link posted user photos, allowing Facebook the ability to collect, analysis, and link individual biometric identifiers associated with user accounts.[46] Even when users learn of social medias growing privacy intrusions, they willfully remain a captive audience instead of ceasing use of the service, because they feel the sites already has a lot of their information and collecting a little more is irrelevant.[47] Photos posted to social media sites provide much more information than just the image. The sites can connect the people in the image with a date, time, and location when the "Geotag" feature on their smart devices are not disabled. This becomes especially disconcerting for SOF members concerned with their image being linked with friends, neighbors, and family members, not to mention the actual location background information on photos taken on overseas deployments.

Social media sites are now actively pursuing user biometric technologies in order to capture individual features and or behavioral characteristics that are unique to the user, advertised as increasing site security, supporting Multi-Factor Authentication (MFA).[48] Sites using MFA enabled security protocols require two forms of information to log into an account, typically a combination of passwords, pins, and or biometric data (i.e. finger print or facial recognition). The individuals unique features or characteristics acts as a "proof of property", functioning as a physically link between the individual and the account being accessed.[49] Jacob Silverman asserts that "Facial recognition offers few obvious benefits and is, by design, inclined to serve the needs of advertisers, intelligence agencies, security contractors, and other potentially untrustworthy actors."[50] But, with the growing use of biometric enabled devices and programs; smart watches, fitness monitors, iPhone finger print reader, or Microsoft Windows 10 – "Hello" facial recognition, just to name a few, users are embracing the new technology and convenience - but at what future cost to privacy?

Finally, the last bastion of individual identity is currently being exploited by companies like, 23andMe.com and ancestryDNA.com, where users voluntarily provide a DNA sample to develop a personal genomic profile in order to map ones family history or identify any genetic predisposition to illness or disease.[51] This burgeoning new business charts personal genomics to "collect, analyze, and share customers genetic data over the internet" for the purpose of easy customer access and to expand branch research services and drug development businesses.[52] The concept of mapping DNA to learn about ones historical past, family origin, ancestral lineage, and ethnic composition is extremely alluring for those pursuing genealogical truth, but also presents a creepy opportunity for companies to collect, share, and or sell customer physical information. Moreover, biometric data is unique to the individual and cannot be changed or reset if the information is compromised, unlike a password or security question. Users just do not realize the amount of information they willingly post or that is aggregated and accessible through social media sites, all under the umbrella of modernity, experience, and convenience. This treasure trove of information represents an irresistible opportunity for nefarious actors to search, access, or hack in order to target or harass general social media users, but can also provide actionable information to specifically target the SOF community, personnel, or their families.

HACKING – LOW RISK, HIGH YEILD

Google did a great job hacking the Web to create search - and then monetizing search with advertising. And Apple did a great job humanizing hardware and software so that formerly daunting computers and applications could become consumer-friendly devices - even a lifestyle brand.[53]

- Douglas Rushkoff, Prof of Media Theory

Over the past decade, nefarious actors (petty or organized criminals, state or non-state actors, or terrorists) have increasingly turned to hacking data bases, through cyber-attacks, to access the mass volumes of public, personal, and financial information accumulated by aggregators, companies, or large

cloud storage farms. Considered a low risk – high yield crime, a skilled hacker can attack secure systems to access sensitive data (social security numbers, names, address, and account or personal information) to harass, target, or commit identity theft from any internet connection in the world with little to no worry of punishment.[54] To further compound the growing problem, data breaches may go undetected for week, months, or even years after the information was initially compromised, giving hackers the opportunity to exploit the information before any corrective action can be taken to prevent or limit the personal or financial injury. Moreover, social media users are unwittingly perpetuating and enabling cyber-attacks by acting as carriers, distributing malicious codes and viruses between web sites infecting up to 30,000 poorly secured sites per day.[55] Below are just a few of the larger, more publicized, hacks and data breaches over the last decade:

- *Veterans Affairs* (VA), data breach in 2006, caused by the theft of an employee's computer exposed 26 million veterans and military personnel, compromising social security numbers, dates of birth, and other personal information. The VA has done little to correct the practice of transmitting unencrypted personal data through unsecure systems.[56]

- *National Archives and Records Administration* (NARA), data breach in 2009, exposed 70 million veterans, compromising social security numbers and personal information. Described as the largest single release of PII in government history at that time.[57]

- *LinkedIn*, hacked in 2012, exposed 117 million users, compromising passwords, email addresses, and personal information, posting 6.5 million on a Russian hacker forum and later offered the rest of the data for sale.[58]

- *Target*, retail store, hack in 2013 exposed 40 million customers, compromising every credit card used across their 1,797 US stores. Credit card information included numbers and names.[59]

- *MySpace*, hack in 2013, exposed 360 million accounts, compromising user email addresses, names, and passwords.[60]

- *Yahoo* hacked twice, 2013 and 2014, exposing 1 billion and 500 million accounts respectfully. Hackers compromised account holder names, dates of birth, phone numbers, and encrypted and unencrypted passwords and security questions to user email accounts.[61]

- *EBay*, hacked in 2014, exposed 145 million customers, compromising all customer names, email addresses, and encrypted passwords.[62]

- *JPMorgan/Chase*, largest bank in America, hack in 2014 exposed 76 million individual account holders and 7 million businesses, compromising credit card and other sensitive personal and corporate information.[63]

- *Home Depot*, retail home improvement store, hack in 2014 exposed 56 million customers, compromising credit card and personal information.[64]

- *Office of Personnel Management* (OPM), government database, hack in 2015 exposed 21.5 million government employees and military personnel, compromising personal information, including security clearance application data submitted on SF-86, clearance level currently held, social security numbers, and DoD employment history.[65]

- *Experian*, world's largest credit report data broker, hack in 2015 exposed 15 million customers, compromising user full names and addresses, including driver's license, social security, and passport numbers.[66]

- *Internal Revenue Service* (IRS), hack in 2015 exposed 700,000 tax payer information, comprising names, social security numbers, and other personal information required to file a false tax return.[67]

- *Friend Finder Networks*, AdultFriendFinder an adult dating site, hack in 2016 exposed over 400 million user accounts, compromising user email addresses, passwords, and registration dates.[68]

- *US Navy*, hack in 2016 exposed more than 134,000 sailors' personal information, compromising names, social security numbers, and other sensitive information.[69]

Although this is only a small sample of the number of data breaches that occurred over the last decade, the total number of accounts compromised and the type of information exposed in just these fourteen events alone are staggering – and the frequency of these events are increasing. From July 2014 to July 2015, the total number of cyber-attacks on large companies increased by forty percent.[70] As technology advances to secure mass information, criminals are identifying vulnerabilities to it for monetary gain, while terrorists use these vulnerabilities as a means to spread propaganda and harass or target those in support of or opposing their ideology.

EXPLOITATION OF MASS INFORMATION BY TERRORISTS

My Muslim brothers, do not underestimate the importance of any piece of information, as simple as it may seem; the mujahedeen, the lions of monotheism, may be able to use it in ways that have not occurred.[71]

-Al-Qaeda communiqué December 2009

American soldiers, we are coming, watch your back!
Isis is already here, we are in your PCs, in each military base.[72]
- United Cyber Caliphate, ISIS Hacking Group

The quotes above highlight that terrorist groups like the Islamic State (ISIS) are actively using social media as a means of influencing, dissuading, and frightening opposition to their extremist ideology. ISIS's ability to leverage technology to perpetrate cyber-attacks, more than any other terrorist organization, have become increasingly sophisticated and have repeatedly called for attacks on Americans at home in retaliation for military actions in the middle east.[73] The United Cyber Caliphate (UCC), a pro-ISIS hacking group, have generated and dispersed several "kill lists", targeting the US military, service members, State and federal law enforcement agencies, federal employees, and general American civilians at large. The UCC "kill lists" have included the names, physical addresses, and email addresses of targeted individuals or general civilians, calling upon ISIS sympathizers (lone-wolves) to attack and "kill them strongly to take revenge for Muslims."[74] On September 25, 2016, Ardit Ferizi, a Kosovo citizen and ISIS sympathizer, was convicted and sentenced to twenty years in prison for providing ISIS with PII on 1,300 US service members and federal employees that he hacked from the computers systems of US based companies.[75] Although, the number of "kill lists" recently generated by extremist organizations are alarming, they are portrayed by government authorities as simply a scare tactic to shock the American society into loosening its resolve to combat extremism, but do not target specific military units or individually identified service

members. As terrorist organizations become increasingly more proficient in exploiting social media as a means to projecting their ideology, they are beginning to refine their targeting.

The relentless publicity and politicization of successful SOF operations over the past decade have increasingly highlighted SOF as the primary forces attacking at the heart of extremist organizations, most notably the operation that killed Osama bin Laden in May 2011. Although, the most visible of all the recently publicized SOF operations, because the operation killed the 9/11 terrorist master mind, once ex-Navy SEAL Robert O'Neill revealed himself in 2014 as the one who pulled the trigger, he immediately became a prime target for all Muslim extremist groups around the world. In 2015, a pro-ISIS Britain posted O'Neill's address in a jihadi online chat room with instructions on how to find and kill him, stating "I leave this info of Robert O'Neill for my brothers in America and Al Qaeda in the U.S., as a number one target to eventually hunt down and kill."[76] O'Neil's apparent rush to cash in on his moment of fame, breaks every SOF code of conduct, ethos, or rule of the "quiet professional", but unfortunately this threat is not his alone. His actions, and those of many other who seek recognition, in public or private circles, provide a starting point for extremists around the world to uncover the digital links between all SOF members, active duty or retired. No matter how small or insignificant a piece of information appears to be (a phone number, an address, even a photo), it absolutely represents a piece of a larger puzzle, that once collectively exposed, represents a very tangible and targetable vulnerability to the SOF community, SOF member, and SOF family.

REVIEW OF DOD AND USSOCOM INTERNET/SOCIAL MEDIA POLCIES

Today's technologies refuse to let people alone, attempting to reconstruct people's past while authoring their future. The need to protect individual rights to lead a full and social life in the face of intrusive technology has never been greater.[77]

-Lori Andrews, Prof of Technology Law

The advances in technology coupled with the accuracy and convenience of high speed access to digital information has transformed the way individuals, society, and the military communicate. Technology will continue to advance and become more and more a part of our everyday lives, but those that work with, and have access to classified material or conduct sensitive overseas operations, particularly SOF, need to understand the threat of exposing operational and personal information. Existing DoD instructions, 8550.01, provides direction for commanders to safeguard and maintain IbC / NIPRNET security supporting operational requirements, while balancing limitations to service members access to communicate on social media sites.[78] The current DoD stance is to maintain service member's first amendment rights, while only limiting IbC access as required to maintain operational capabilities. DoD policy primarily focuses on institutional OPSEC, providing limited official guidance regulating individual social media use other than not exposing PII. To prevent unauthorized PII release and increase OPSEC awareness, DoD requires all service members, employees, and contractors to complete annual PII / OPSEC training to maintain access to DoD NIPRNET systems.

USSOCOM adheres to DoD IbC policies, but has identified advancements in technology and the rapidly growing us of social media not only represents a threat to institutional OPSEC effecting overseas operations, but also presents a mounting vulnerability to the SOF community, SOF members, and SOF families at home. In addition to the required annual DoD training requirements, the USSOCOM IdM branch provides social media awareness and identity management training to increase the SOF communities understanding of the vulnerabilities

associated with unguarded social media usage.[79] The mission of the IdM branch is to identify and correct gaps in policies, procedures, and training to mitigate data breaches, cyber-attacks, release of PII, and media or criminal exploitation of SOF members thru digital means.[80] Additionally, IdM branch generates and provides "Smart Cards", designed to deter, detect, defend, and avoid compromising personal information when using personal smart devices and social media sites. The "Smart Cards" provide detailed instructions to maximize security settings on social media sites, smart devices, and home computers to limit or avoid device tracking, turn off photo metadata tagging, and limit overexposure of personal information. Moreover, due to USSOCOMs proactive approach to increase social media awareness, active duty SOF members and SOF DoD employees have become more mindful of the potential operational and personal security vulnerabilities associated with unguarded social media usage, leaving only one SOF community audience remaining in need of awareness training – the family.

RECOMMENDATTIONS TO MITIGATE SOF VULNERABILTIES

DoD, particularly USSOCOM service members, employees, and contractors understanding of social media vulnerabilities have increased significantly over recent years due to repeated mandatory training and access to available resources, but SOF families are not required to obtain the same level of awareness. Arguably the families are and will always be the most difficult to reach and convince when implementing new policies or guidance, since family members are civilians and not subject to DoD regulations, leaving DoD with limited to no control over family member's actions. With limited options or ability to enforce mandatory training or awareness, it is now incumbent on the service member to take the lead in educating family members on the hazards of unguarded social media "hyper-connectivity" that can inadvertently expose the families and the SOF community to unnecessary social media exposure.

USSOCOM would be well served to focus resources towards awareness opportunities and training aids specifically targeting SOF family social media and digital identity wellness. Generating family specific training aids and products need to focus relevant and age appropriate material to increase social media awareness, while being short in duration and thought-provoking enough to entice interest and consumption. Products can range from simple short message fliers or handouts to short video infomercials addressing a wide range of social media, internet, and digital identity concerns and actions to mitigate vulnerabilities. Additionally, products should be generated that describe actual or fictitious scenarios that led to or could lead to identify theft, harassment, or targeting to include safe practice solutions to counter the potential threats. Finally, USSOCOM and subordinate commands need to synchronize and unify family awareness and training efforts to effectively and consistently message the growing social media concern, thereby reducing SOF community social media vulnerabilities.

SOF service members have a professional and personal obligation to educate their families on what is acceptable and what is not acceptable when it comes to disseminating or posting any information associated with the SOF community, work related details, or SOF activities and associations. This starts with reinforcing the return of the "Quiet Professional" persona by limiting and not advertising the nature of one's work in either a personal or social media setting. Service members are encouraged to leverage DoD, USSOCOM, MWR, and Family Readiness Group (FRG) training assets to educate family members on how to enable security settings on computers, smart devices, and social media sites to include sharing real social media case studies explaining what went wrong and how to prevent it from happening the them. Additionally, SOF members need to take an active role in guiding their children's usage of smart devices and electronic media while understanding the generational gaps, paternalistic

frictions, naïve expectations, and evolving technology requiring continual attention, monitoring, and patience.

Advances in modern communication technology have transformed the way society interacts, communicate, learns, and expresses emotions, interests, and dreams. Beyond the conveniences of incessant connectivity, modernity presents an opportunity for those that will take advantage of those freely and openly participating in the endless flow of information. The goal is for all SOF members to actively manage their identities on social media and not blindly participate with the masses as they are herded up as the commodity they have become in the digital world.

LIST OF ACRONYMS

CIO	Chief Information Officer
CPM	Communication Privacy Management Theory
DoD	Department of Defense
DTIC	Defense Technical Information Center
FRG	Family Readiness Group
GPS	Global Positioning System
GRC	Gray Research Center
GWI	GlobalWebIndex
IbC	Internet-based Capabilities
IdM	Identity Management
ISIS	Islamic State
MFA	Multi-Factor Authentication
MWR	Moral, Welfare, and Recreation
NIPRNET	Non-Classified Internet Protocol Router Network
OPSEC	Operational Security
PII	Personally Identifiable Information
SNS	Social Networking Services
SOF	Special Operations Forces
UCC	United Cyber Caliphate
USMCU	United States Marine Corps University
USSOCOM	United States Special Operations Command

NOTES

[1] Jaron Lanier, "*Who Owns the Future",* (New York: Simon & Schuster: 2103), 15.

[2] U.S. Chief Information Officer and the Federal CIO Council, *"Privacy Best Practices for Social Media"*, (July 2013), https://cio.gov/wp-content/uploads/downloads/2013/07/Privacy-Best-Practices-for-Social-Media.pdf, 2.

[3] Brian Solis, (February 25, 2011), http://www.briansolis.com/2011/02/behaviorgraphics-discovering-the-me-in-social-media/.

[4] Solis, (February 25, 2011).

[5] Gabriel Weimann, *"Terrorism in Cyberspace: The Next Generation"*, (Washington, D.C., Woodrow Wilson Center Press, 2015), 134.

[6] Mark Pribish, *"U.S. military, vets often ID-theft targets"*, (The Arizona Republic, June 19, 2014), Http://www.azcentral.com/story/money/business/2014/06/19/us-military-vets-often-theft-targets/11014519/.

[8] Lanier,*1-2*.

[9] Sandra Petronio, "Communication Privacy Management Theory", *A First Look at Communication Theory*, 9th edition (Chapter 12), 151.

[10] Gabriel Weimann, *"Terrorism in Cyberspace: The Next Generation"*, 134.

[11] Lori Andrews, *"I Know Who You Are and I Saw What You Did: Social Networks and the death of privacy"*, (New York: Free Press, 2011), 3.

[12] Jacob Silverman, video discussion, *"Terms of Service: Social Media and the Price of Constant Connection"* (YouTube video, June 24, 2015), 47:35, https://www.youtube.com/watch?v=jhaMtnjGhhc.

[13] US Deputy Secretary of Defense, Directive-Type Memorandum (DTM) 09-026 – *Responsible and Effective use of Internet-based Capabilities*, February, 25, 2010, https://www.defense.gov/Portals/1/Documents/DTM%2009-026.pdf.

[14] US Department of Defense, Instruction 8550.01, *DoD Internet Services and Internet-Based Capabilities*, September 11,2012, http://www.dtic.mil/whs/directives/corres/pdf/855001p.pdf.

[15] Joel Stein, *"Data Mining: How Companies Now Know Everything About You"*, (Time Magazine, March 10, 2011) http://content.time.com/time/magazine/article/0,9171,2058205,00.html.

[16] Susan B. Barnes, *"A Privacy Paradox: Social Networking in the United States"*, (First Monday Peer-Reviewed Journal on the Internet, September 4, 2006), http://firstmonday.org/article/view/1394/1312_2.

[17] James R. Beniger, "*The Control Revolution: Technological and Economic Origins of the Information Society",* (Cambridge, Mass.: Harvard University Press, 1986). 436.

[18] Stein.

[19] Ibid.

[20] CSC, Big Data Infographic (2012), http://assets1.csc.com/insights/downloads/CSC_Infographic_Big_Data.pdf.

[21] TurboFuture, *"The Dangers of Social Networking"*, (April 29, 2016), https://turbofuture.com/internet/The-Dangers-of-Social-Networking-Why-you-need-to-be-careful.

[22] Andrews, 9.

[23] David Lazarus, *"You won't find Spokeo founder included on his 'people search' site"*, (Los Angeles Times, June 8, 2010), http://articles.latimes.com/2010/jun/08/business/la-fiw-lazarus-20100608.

[24] GlobalWebIndex, *"GWI Social Summary Report"*, (Q1 2015), https://www.globalwebindex.net/hs-fs/hub/304927/file-2812772150-pdf/Reports/GWI_Social_Summary_Report_Q1_2015.pdf., 1-3.

[25] GlobalWebIndex.

[26] Ibid.

[27] Barnes.

[28] Petronio, 151.

[29] Ibid, 151.

[30] R.M. McLaren, *"Emotions, Communicative responses, and relational consequences of boundary turbulence"*. Journal of Social and Personal Relationships. (August 2013). 30 (5): 606–626

[31] Dennis Desmond, Identity Management Branch Chief at USSOCOM, Phone interview by LCDR J.H. Hora, January 11, 2017.

[32] Brian Solis, *"Brian Solis, 10 Quotes on the Future of Business"* (June 9, 2014), http://www.briansolis.com/2014/06/10-quotes-future-business/.

[33] Cross, Michael. *"Social Media Security, Leveraging Networking While Mitigating Risk",* (New York: Elservier, 2014), 22.

[34] Danny Sullivan. *"Google Handles at Least 2 Trillion Searches per Year"*, Search Engine Land, (May 24, 2016), http://searchengineland.com/google-now-handles-2-999-trillion -searches-per-year-250247.

[35] US Securities and Exchange Commission, Google - Annual Report, Form 10-K, (December 31, 2015), https://www.sec.gov/Archives/edgar/data/1288776/000165204416000012/goog10-k2015., 21.

[36] Jacob Silverman, *"Terms of Service: Social Media and the Price of Constant Connection."* (New York: HarperCollins Publishers, 2015), 7.

[37] Zephoria Digital Marketing, *"The Top 20 Valuable Facebook Statistics"*, (December 2016), https://zephoria.com/top-15-valuable-facebook-statistics/.

[38] Jitender Miglani, *"Facebook Revenues, Profits, and Users Growth Analysis 2015"*, Revenues and Profits, (January 28, 2016), http://revenuesandprofits.com/facebook-revenues -profits-and-users-growth-analysis-2015/.

[39] Forbes Magazine, *"The World's Billionaires"*, (December 30, 2016), http://www.forbes.com /billionaires/list/.

[40] Facebook, *"Facebook – Company Info"*, (December 30, 2016) http://newsroom.fb.com/ company-info/.

[41] Federal Trade Commission, In the Matter of Facebook, Inc. and the Facial Identification of Users (June 10, 2011), https://epic.org/privacy/facebook/EPIC_FB_FR_FTC_Complaint _06_10_11.pdf., 23.

[42] Steve Toth, *"65 Facebook Acquisitions – The Complete List (2017)!"*, October 26, 2016, https://www.techwyse.com/blog/infographics/65-facebook-acquisitions-the-complete-list-infographic/; Jay Green, *"Microsoft to Acquire LinkedIn for $26.2 Billion"*, The Wall Street Journal, June 14, 2016, http://www.wsj.com/articles/microsoft-to-acquire-linkedin-in-deal-valued-at-26-2-billion-1465821523.

[43] Beth Willington, *"What Facebook Fails to Recognize"*, The Guardian (June 14, 2011), https://www.theguardian.com/commentisfree/cifamerica/2011/jun/14/facebook-facial-recognition-software.

[44] Kris Carlon, *"(Update: UK data sharing paused) WhatsApp under fire for sharing user data with Facebook"*, Android Authority (November 6, 2016), http://www.androidauthority.com/whatsapp-sharing-user-data-facebook-725347/.

[45] Federal Trade Commission, In the Matter of Facebook, Inc. and the Facial Identification of Users (June 10, 2011), 8.

[46] Ibid, 9-10.

[47] Ibid, 9-10.

[48] Thomas P. Keenan, *"Hidden Risks of Biometric Identifiers and How to Avoid Them"*, Black Hat 2015, (October 1, 2015), https://www.ftc.gov/system/files/documents/public_comments/2015/10/00070-98117.pdf.

[49] David Chek Ling Ngo, Andrew Beng Jin Teoh, and Jiankun Hu, *"Biometric Security"* (New Castle, Cambridge Scholars Publishing, 2015), Preface.

[50] Silverman, xii.

[51] Ibid, 305.

[52] Ravi Vij, *"How 23andMe Makes Money? Understanding 23andMe Business Model"*, Revenues and Profits, (March 21, 2016), http://revenuesandprofits.com/how-23andme-makes-money-understanding-23andme-business-model/.

[53] Douglas Rushkoff, BrainyQuote.com, Xplore Inc, 2017. https://www.brainyquote.com/quotes/quotes/d/douglasrus585208.html, accessed January 8, 2017.

[54] Kevin Mitnick. BrainyQuote.com, Xplore Inc, 2017. https://www.brainyquote.com/quotes/quotes/k/kevinmitni469445.html, accessed January 8, 2017.

[55] James Lyne, *"30,000 Web Sites Hacked A Day. How Do You Host Yours?"*, Forbes, (September 6, 2013), http://www.forbes.com/sites/jameslyne/2013/09/06/30000-web-sites-hacked-a-day-how-do-you-host-yours/#57e2e0d63a8c.

[56] Mark Flatten, *"UPDATED! Chinese, other nations hacked VA computers, officials can't account for everything stolen"*, The Washington Examiner, (June 4, 2013), http://www.washingtonexaminer.com/updated-chinese-other-nations-hacked-va-computers-officials-cant-account-for-everything-stolen/article/2531106

[57] Ryan Singel, "*Probe Targets Archives' Handling of Data on 70 Million Vets",* Wired, (October 1, 2009), https://www.wired.com/2009/10/probe-targets-archives-handling-of-data-on-70-million-vets/.

[58] Sarah Perez, *"117 million LinkedIn emails and passwords from a 2012 hack just got posted online"* Tech Crunch (May 18, 2016), https://techcrunch.com/2016/05/18/117-million-linkedin-emails-and-passwords-from-a-2012-hack-just-got-posted-online/.

[59] Michael Riley, Benjamin Elgin, Dune Lawrence, and Carol Matlack, *"Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It"*, Bloomberg, (March 17, 2014), https://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data.

[60] Brian Barrett, *"Hack Brief: Your Old Myspace Account Just Came Back to Haunt You"*, Wired (May 31, 2016), https://www.wired.com/2016/05/hack-brief-old-myspace-account-just-came-back-haunt/.

[61] Vindu Goel and Nicole Perlroth, *"Yahoo Says 1 Billion User Accounts Were Hacked"*, The New York Times, (December, 14, 2016), http://www.nytimes.com/2016/12/14/technology/yahoo-hack.html?_r=1.

[62] Jim Finkle and Deepa Seetharaman, *"Cyber Thieves Took Data On 145 Million eBay Customers By Hacking 3 Corporate Employees",* Business Insider, (May 27, 2014), http://www.businessinsider.com/cyber-thieves-took-data-on-145-million-ebay-customers-by-hacking-3-corporate-employees-2014-5.

[63] Elisabeth Weise, *"JP Morgan Reveals Data Breach Affected 76 Million Households*", USATODAY, (October 2, 2014), http://www.usatoday.com/story/tech/2014/10/02/jp-morgan-security-breach/16590689/.

[64] Robin Sidel, *"Home Depot's 56 Million Card Breach Bigger Than Target's"*, The Wall Street Journal, (September 18, 2014), http://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571.

[65] Jim Scuitto, *"OPM Government Data Breach Impacts 21.5 Million"*, CNN, (July 10, 2015), http://www.cnn.com/2015/07/09/politics/office-of-personnel-management-data-breach-20-million/.

[66] Sam Thielman, *"Experian hack exposes 15 million people's personal information"*, The Guardian, (October 1, 2015), https://www.theguardian.com/business/2015/oct/01/experian-hack-t-mobile-credit-checks-personal-information.

[67] Kevin McCoy, *"Cyber hack got access to over 700,000 IRS accounts"*, USA TODAY, (February 26, 2016), http://www.usatoday.com/story/money/2016/02/26/.cyber-hack-gained-access-more-than-700000-irs-accounts/80992822/.

[68] Rob Price, *"Over 400 million user accounts were stolen after an adult website was hacked"*, Business Insider, (November 14, 2016), http://www.businessinsider.com/adult-dating-site-adultfriendfinder-hacked-400-million-user-accounts-stolen-october-2016-11.

[69] David B. Larter, *"Personal data for more than 134,000 sailors was breached, Navy says"*, NavyTimes, (November 23, 2016), https://www.navytimes.com/articles/data-breach-exposes-more-than-100-000-sailors-information.

[70] Thomas Lewis, *"'Data-Hack Fatigue' Exists – Here's How to Fight it"*, Information Security Blog, (July 1, 2015), http://www.lbmcinformationsecurity.com/blog/data-hack-fatigue-exists-heres-how-to-fight-it.

[71] Kate Wiltrout, *"Islamist Web sites discuss attacks on U.S. warships"*, The Virginia Pilot, (January 8, 2010), http://pilotonline.com/news/military/islamist-web-sites-discuss-attacks-on-u-s-warships/article_55c25ff9-302d-57a2-821c-52079485f15b.html.; Navy, VP-4, Operational Security (OPSEC) and Social Networking brief, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwju2bCZs8LRAhULIcAKHa1eCE4QFggaMAA&url=http%3A%2F%2Fwww.vp4.navy.mil%2Fdeployment%2F6OPSECandSocialNetworking.ppt&usg=AFQjCNH6sTpc5oMRSUHoFQqgN54mBhmT2A&bvm=bv.144224172,d.ZGg&cad=rja.

[72] Spencer Ackerman, *"US Central Command Twitter account hacked to read 'I love you Isis'"*, The Guardian, (January 12, 2015), https://www.theguardian.com/us-news/2015/jan/12/us-central-command-twitter-account-hacked-isis-cyber-attack.

[73] Mark Pomerleau, *"State vs. non-state hackers: Different tactics, equal threat?"*, Defense Systems, (August 17, 2015), https://defensesystems.com/articles/2015/08/17/cyber-state-vs-non-state-haclers-tactics.aspx.

[74] Gilad Shiloach, *"New ISIS 'Kill' List Claims to Target Thousands of Americans"*, Vocativ, (June 8, 2016), http://www.vocativ.com/326931/new-isis-kill-list-claims-to-target-thousands-of-americans/.

[75] Evan Perez, Catherine E. Shoichet and Wes Bruer, *"Hacker who allegedly passed U.S. military data to ISIS arrested in Malaysia"*, CNN, (October 19, 2015), http://www.cnn.com/2015/10/15/politics/malaysian-hacker-isis-military-data/.; Rachel Weiner, *"Hacker who sent 'kill list' of U.S. military personnel to ISIS: 'I feel so bad'"*, The Washington Post, (September 23, 2016), https://www.washingtonpost.com/local/public-safety/hacker-who-sent-kill-list-of-us-military-personnel-to-islamic-state-i-feel-so-bad/2016/09/23/dc0ba0ea-8196-11e6-b002-307601806392_story.html?utm_term=.ad2a149a927c.

[76] Oriana Pawlyk, *"Former Navy SEAL Robert O'Neill, who said he killed bin Laden, 'number one' ISIS target"*, MilitaryTimes, (October 6, 2015), http://www.militarytimes.com/story/military/2015/10/06/former-seal-robert-oneill-number-one-isis-target/73439906/.

[77] Andrews, 59.

[78] US Department of Defense, Instruction 8550.01, *DoD Internet Services and Internet-Based Capabilities*, September 11,2012.

[79] Dennis Desmond, Identity Management Branch Chief at USSOCOM, Phone interview by LCDR J.H. Hora, January 11, 2017.

[80] Ibid.

ILLISTRATIONS

BIBLIOGRAPHY

Ackerman, Spencer. *"US Central Command Twitter account hacked to read 'I love you Isis'"*, The Guardian, January 12, 2015), https://www.theguardian.com/us-news/2015/jan/12/us-central-command-twitter-account-hacked-isis-cyber-attack.

Andrews, Lori. *"I Know Who You Are and I Saw What You Did: Social Networks and the death of privacy"* New York: Free Press, 2011.

Barnes, Susan B. *"A Privacy Paradox: Social Networking in the United States"* First Morning Peer-Reviewed Journal on the Internet, September 4, 2006), http://firstmonday.org/article/view/1394/1312_2.

Barrett, Brian. *"Hack Brief: Your Old Myspace Account Just Came Back to Haunt You"*, Wired May 31, 2016, https://www.wired.com/2016/05/hack-brief-old-myspace-account-just-came-back-haunt/.

Beniger, James R. "*The Control Revolution: Technological and Economic Origins of the Information Society."* Cambridge, Mass.: Harvard University Press, 1986.

Carlon, Kris. *"(Update: UK data sharing paused) WhatsApp under fire for sharing user data with Facebook"* Android Authority, November 6, 2016, http://www.androidauthority.com/whatsapp-sharing-user-data-facebook-725347/.

Cross, Michael. *"Social Media Security, Leveraging Networking While Mitigating Risk."* New York: Elservier, 2014.

Facebook. *"Facebook – Company Info"*, December 30, 2016, http://newsroom.fb.com/company-info/.

Federal Trade Commission. *"In the Matter of Facebook, Inc. and the Facial Identification of Users"* June 10, 2011, https://epic.org/privacy/facebook/EPIC_FB_FR_FTC_Complaint_06_10_11.pdf., 23.

Finkle, Jim and Deepa Seetharaman. *"Cyber Thieves Took Data On 145 Million eBay Customers by Hacking 3 Corporate Employees"* Business Insider, May 27, 2014, http://www.businessinsider.com/cyber-thieves-took-data-on-145-million-ebay-customers-by-hacking-3-corporate-employees-2014-5.

Flatten, Mark. *"UPDATED! Chinese, other nations hacked VA computers, officials can't account for everything stolen"*, The Washington Examiner, June 4, 2013, http://www.washingtonexaminer.com/updated-chinese-other-nations-hacked-va-computers-officials-cant-account-for-everything-stolen/article/2531106.

Forbes Magazine. *"The World's Billionaires"*, December 30, 2016, http://www.forbes.com./billionaires/list/.

GlobalWebIndex. *"GWI Social Summary Report"*, Q1 2015, https://www.globalwebindex.net/hs-fs/hub/304927/file-2812772150-pdf/Reports/GWI_Social_Summary_Report_Q1_2015.pdf.

Goel, Vindu and Nicole Perlroth. *"Yahoo Says 1 Billion User Accounts Were Hacked"*, The New York Times, December, 14, 2016, http://www.nytimes.com/2016/12/14/technology/yahoo-hack.html?_r=1.

Green, Jay. *"Microsoft to Acquire LinkedIn for $26.2 Billion."* The Wall Street Journal, June 14, 2016, http://www.wsj.com/articles/microsoft-to-acquire-linkedin-in-deal-valued-at-26-2-billion-1465821523.

Keenan, Thomas P. *"Hidden Risks of Biometric Identifiers and How to Avoid Them"*, Black Hat 2015, https://www.ftc.gov/system/files/documents/public_comments/2015/10/00070-98117.pdf.

Lanier, Jaron. *"Who Owns the Future."* New York: Simon & Schuster: 2013.

Larter, David B. *"Personal data for more than 134,000 sailors was breached, Navy says"*, NavyTimes, November 23, 2016, https://www.navytimes.com/articles/data-breach-exposes-more-than-100-000-sailors-information.

Lazarus, David. *"You won't find Spokeo founder included on his 'people search' site"* Los Angeles Times, June 8, 2010, http://articles.latimes.com/2010/jun/08/business/la-fiw-lazarus-20100608.

Lewis, Thomas. *"'Data-Hack Fatigue' Exists – Here's How to Fight it"*, Information Security Blog, July 1, 2015, http://www.lbmcinformationsecurity.com/blog/data-hack-fatigue-exists-heres-how-to-fight-it.

Lyne, James. *"30,000 Web Sites Hacked a Day. How Do You Host Yours?"*, Forbes, September 6, 2013, http://www.forbes.com/sites/jameslyne/2013/09/06/30000-web-sites-hacked-a-day-how-do-you-host-yours/#57e2e0d63a8c.

McCoy, Kevin. *"Cyber hack got access to over 700,000 IRS accounts"*, USA TODAY, February 26, 2016, http://www.usatoday.com/story/money/2016/02/26/cyber-hack-gained-access-more-than-700000-irs-accounts/80992822/.

McLaren, R.M. "Emotions, Communicative responses, and relational consequences of boundary turbulence". *Journal of Social and Personal Relationships*. August 2013. 30 (5): 606–626

Miglani, Jitender. *"Facebook Revenues, Profits, and Users Growth Analysis 2015"*, Revenues and Profits, January 28, 2016, http://revenuesandprofits.com/facebook-revenues-profits-and-users-growth-analysis-2015/.

Mitnick, Kevin. BrainyQuote.com, Xplore Inc, 2017. https://www.brainyquote.com/quotes/quotes/k/kevinmitni469445.html, accessed January 8, 2017.

Navy. VP-4, Operational Security (OPSEC) and Social Networking brief, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwju2bCZs8LRAhULIcAKHa1eCE4QFggaMAA&url=http%3A%2F%2Fwww.vp4.navy.mil%2Fdeployment%2F6OPSECandSocialNetworking.ppt&usg=AFQjCNH6sTpc5oMRSUHoFQqgN54mBhmT2A&bvm=bv.144224172,d.ZGg&cad=rja.

Ngo, David Chek Ling., Andrew Beng Jin Teoh, and Jiankun Hu, *"Biometric Security"* New Castle, Cambridge Scholars Publishing, 2015, Preface.

Pawlyk, Oriana. *"Former Navy SEAL Robert O'Neill, who said he killed bin Laden, 'number one'ISIS target"*, MilitaryTimes, (October 6, 2015), http://www.militarytimes.com/story/military/2015/10/06/former-seal-robert-oneill-number-one-isis-target/73439906/.

Perez, Evan., Catherine E. Shoichet and Wes Bruer, *"Hacker who allegedly passed U.S. military data to ISIS arrested in Malaysia"*, CNN, October 19, 2015, http://www.cnn.com/2015/10/15/politics/malaysian-hacker-isis-military-data/.

Perez, Sarah. *"117 million LinkedIn emails and passwords from a 2012 hack just got posted online"* Tech Crunch May 18, 2016, https://techcrunch.com/2016/05/18/117-million-linkedin-emails-and-passwords-from-a-2012-hack-just-got-posted-online/.

Petronio, Sandra. "Communication Privacy Management Theory", *A First Look at Communication Theory*, 9th edition (Chapter 12

Pomerleau, Mark. *"State vs. non-state hackers: Different tactics, equal threat?"*, Defense Systems, August 17, 2015, https://defensesystems.com/articles/2015/08/17/cyber-state-vs-non-state-haclers-tactics.aspx.

Pribish, Mark. *"U.S. military, vets often ID-theft targets."* The Arizona Republic, June 19, 2014, http://www.azcentral.com/story/money/business/2014/06/19/us-military-vets-often-theft-trgets/11014519/.

Price, Rob. *"Over 400 million user accounts were stolen after an adult website was hacked"*, Business Insider, November 14, 2016, http://www.businessinsider.com/adult-dating-site-adultfriendfinder-hacked-400-million-user-accounts-stolen-october-2016-11.

Riley, Michael, Benjamin Elgin, Dune Lawrence, and Carol Matlack, *"Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It"*, Bloomberg, March 17, 2014, https://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data.

Rushkoff, Douglas. BrainyQuote.com, Xplore Inc, 2017. https://www.brainyquote.com/quotes /quotes/d/douglasrus585208.html, accessed January 8, 2017.

Scuitto, Jim. *"OPM Government Data Breach Impacts 21.5 Million"*, CNN, July 10, 2015, http://www.cnn.com/2015/07/09/politics/office-of-personnel-management-data-breach-20-million/.

Shiloach, Gilad. *"New ISIS 'Kill' List Claims to Target Thousands of Americans"*, Vocativ, June 8, 2016, http://www.vocativ.com/326931/new-isis-kill-list-claims-to-target-thousands-of-americans/.

Sidel, Robin *"Home Depot's 56 Million Card Breach Bigger Than Target's"*, The Wall Street Journal, September 18, 2014, http://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571.

Silverman, Jacob. *"Terms of Service: Social Media and the Price of Constant Connection."* New York: HarperCollins Publishers, 2015.

Silverman, Jacob. video discussion, *"Terms of Service: Social Media and the Price of Constant Connection"* YouTube video, June 24, 2015, 47:35, https://www.youtube.com/ watch?v=jhaMtnjGhhc.

Solis, Brain. http://www.briansolis.com/2014/06/10-quotes-future-business/.

Singel, Ryan. *"Probe Targets Archives' Handling of Data on 70 Million Vets",* Wired, October 1, 2009, https://www.wired.com/2009/10/probe-targets-archives-handling-of-data-on-70-million-vets/.

Stein, Joel *"Data Mining: How Companies Now Know Everything About You."* Time Magazine, March 10, 2011. http://content.time.com/time/magazine/article/0,9171,2058205,00.html.

Sullivan, Danny. *"Google Handles at Least 2 Trillion Searches per Year"*, Search Engine Land, May 24, 2016, http://searchengineland.com/google-now-handles-2-999-trillion-searches-per-year-250247.

Thielman, Sam. *"Experian hack exposes 15 million people's personal information"*, The Guardian, October 1, 2015, https://www.theguardian.com/business/2015/oct/01/ experian-hack-t-mobile-credit-checks-personal-information.

Toth, Steve. *"65 Facebook Acquisitions – The Complete List (2017)!"* October 26, 2016, https://www.techwyse.com/blog/infographics/65-facebook-acquisitions-the-complete-list-infographic/;

TurboFuture, *"The Dangers of Social Networking"* April 29, 2016, https://turbofuture.com/ internet/The-Dangers-of-Social-Networking-Why-you-need-to-be-careful.

US Chief Information Officer and the Federal CIO Council, *"Privacy Best Practices for Social Media"* July 2013, https://cio.gov/wp-content/uploads/downloads/2013/07/Privacy-Best-Practices-for-Social-Media.pdf, 2.

US Department of Defense, Instruction 8550.01, *DoD Internet Services and Internet-Based Capabilities*, September 11, 2012, http://www.dtic.mil/whs/directives/corres/pdf/855001p.pdf.

US Deputy Secretary of Defense, Directive-Type Memorandum (DTM) 09-026 – *Responsible and Effective use of Internet-based Capabilities*, February, 25, 2010, https://www.defense.gov/Portals/1/Documents/DTM%2009-026.pdf.

US Securities and Exchange Commission, Google - Annual Report, Form 10-K, December 31, 2015, https://www.sec.gov/Archives/edgar/data/1288776/000165204416000012/goog10-k2015.

Vij, Ravi. *"How 23andMe Makes Money? Understanding 23andMe Business Model"*, Revenues and Profits, March 21, 2016, http://revenuesandprofits.com/how-23andme-makes-money-understanding-23andme-business-model/.

Weimann, Gabriel *"Terrorism in Cyberspace: The Next Generation."* Washington, D.C., Woodrow Wilson Center Press, 2015.

Weiner, Rachel. *"Hacker who sent 'kill list' of U.S. military personnel to ISIS: 'I feel so bad'"*, The Washington Post, September 23, 2016, https://www.washingtonpost.com/local/public-safety/hacker-who-sent-kill-list-of-us-military-personnel-to-islamic-state-i-feel-so-bad/2016/09/23/dc0ba0ea-8196-11e6-b002-307601806392_story.html?utm_term=.ad2a149a927c.

Weise, Elisabeth. *"JP Morgan Reveals Data Breach Affected 76 Million Households*", USATODAY, October 2, 2014, http://www.usatoday.com/story/tech/2014/10/02/jp-morgan-security-breach/16590689/.

Willington, Beth. *"What Facebook Fails to Recognize"* The Guardian, June 14, 2011, https://www.theguardian.com/commentisfree/cifamerica/2011/jun/14/facebook-facial-recognition-software.

Wiltrout, Kate. *"Islamist Web sites discuss attacks on U.S. warships"*, The Virginia Pilot, January 8, 2010, http://pilotonline.com/news/military/islamist-web-sites-discuss-attacks-on-u-s-warships/article_55c25ff9-302d-57a2-821c-52079485f15b.html.

Zephonria Digital Marketing. "The Top 20 Valuable Facebook Statistics", December 2016, https://zephoria.com/top-15-valuable-facebook-statistics/.