

Impact of Cybervetting on Job Seekers' Social Media Use and Identity Creation

Courtney Powers
Marquette University

Recommended Citation

Powers, Courtney, "Impact of Cybervetting on Job Seekers' Social Media Use and Identity Creation" (2017). *Master's Theses (2009 -)*. 409.
http://epublications.marquette.edu/theses_open/409

THE IMPACT OF CYBERVETTING ON JOB
SEEKERS' SOCIAL MEDIA USE AND
IDENTITY CREATION

by

Courtney J. Powers, B.A.

A Thesis submitted to the Faculty of the Graduate School,
Marquette University,
in Partial Fulfillment of the Requirements for the Degree Master of Arts

Milwaukee, Wisconsin

May 2017

ABSTRACT
THE IMPACT OF CYBERVETTING ON JOB
SEEKERS' SOCIAL MEDIA USE AND
IDENTITY CREATION

Courtney J. Powers, B.A.

Marquette University, 2017

Social media has become an integral part of connecting with others and sharing personal information. As more individuals use social media to express themselves, organizations have begun using these same sites to make hiring decisions in a process called cybervetting. Although some researchers suggest that cybervetting has consequences for self-expression, currently little research has explored how cybervetting impacts job seekers' social media use and identity creation. Accordingly, this study uses quantitative and qualitative methods to explore how cybervetting impacts job seekers' social media use and online identity creation. By surveying job-seeking social media users, this study measures the relationships between social media use, concern for cybervetting, Communication Privacy Management and facework behaviors, and social media privacy tools. The results from the survey indicate a relationship between social media use and concern for cybervetting, a heavy use of social media privacy tools, and real accounts of social media behavior changes due to cybervetting, but do not show a direct relationship between a concern for cybervetting and Communication Privacy Management and facework behaviors. Although the results point to conflicting findings, this study sheds light on the evolving nature of cybervetting, social media use, and its impact on online identity creation, emphasizing a call for future research.

ACKNOWLEDGEMENTS

Courtney J. Powers, B.A.

I would like to express my sincere gratitude to my thesis advisor, Dr. Scott D'Urso, for his continuous support and invaluable guidance during my thesis project. I would also like to thank the rest of my thesis committee, Dr. Sarah Feldner and Dr. Kerry Egdorf, for their incredible insight and encouragement. All three of these amazing mentors were instrumental in instilling in me a passion for organizational communication. Lastly, I would like to thank my family for their unwavering love and support.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS i

LIST OF TABLES iv

CHAPTER

I. INTRODUCTION 1

II. REVIEW OF LITERATURE 3

 A. Background of Cybervetting 3

 B. How Job Seekers Craft Their Online Identities 5

 C. How Organizations Use Cybervetting 10

 D. Consequences of Cybervetting 14

III. METHODOLOGY 20

 A. Participants and Procedures 20

 B. Measures 22

 i. Social Media Intensity Scale 22

 ii. CPM Social Media Scale 23

 iii. Technological Privacy Tools Measure 24

 iv. Concern for Cybervetting Measure 25

IV. RESULTS 26

V. DISCUSSION 33

 A. Limitations & Future Directions 42

 B. Conclusion 44

VI. BIBLIOGRAPHY 46

VII. APPENDIX A 51

VIII. APPENDIX B65

IX. APPENDIX C 68

X. APPENDIX D 71

XI. APPENDIX E 74

XII. APPENDIX F77

LIST OF TABLES

Table 1: Participant Demographics 21

Table 2: Correlations Between Key Variables 27

Chapter One: Introduction

New advances in technology are transforming the hiring process and changing the way individuals create their identities online. In recent years, the popularity of social media has skyrocketed, with social networking websites (SNS) like Facebook, LinkedIn, and Twitter accumulating millions of active users (Global social networks, 2015). Now, more than ever, people are using these social media outlets to communicate with others and share their identities and personal lives, while organizations are using these same websites to research prospective employees to make hiring decisions in a process called cybervetting (Ghoshray, 2012; Clark & Roberts, 2010; Berkelaar, 2010).

According to Berkelaar (2010), cybervetting refers to the practice of employers obtaining information about individuals from informal, non-institutional, online sources to inform hiring decisions. Millions of people are using SNS to connect and share with others, while employers are using these same sites as a source of background information on job applicants through cybervetting (Clark & Roberts, 2010). Because viewing an individual's social media activities may enable employers to gain valuable insight into an applicant's behavior, cybervetting "has become the norm as opposed to an exception" (Ghoshray, 2012, p. 533).

Due to the popularity of social media and cybervetting, it is important to understand how cybervetting is being used by organizations and the influence it has on individuals. Some employers view cybervetting as a key selection process that allows them to conduct due diligence and eliminate risk (Ghoshray, 2012). Perry (2015) suggests that cybervetting is popular because people may feel comfortable saying or revealing things that allow others to gain insight into their attitudes toward a variety of things,

including work ethics, politics, alcohol, and/or drugs. However, the use of SNS to uncover information about an applicant can also be viewed as a violation of privacy, and may, in fact, influence the way in which job seekers portray themselves online (Brandenburg, 2007). Because employers are using SNS to gather information for their hiring decisions, some applicants feel as though their freedom of speech and right to privacy are being violated. Additionally, some job candidates feel as though their personal social media accounts, which display their lives and self-created identities, are being judged by employers. Accordingly, this research will examine how the use of cybervetting influences job seekers' identity creation and behavior on SNS.

Chapter Two: Review of Literature

Background of Cybervetting

To begin to explore how organizations' use of cybervetting influences how job seekers create their identity on SNS, it is key to understand cybervetting and how it contrasts with traditional methods of making hiring and selection decisions. According to Berkelaar (2010), cybervetting occurs when employers acquire information about candidates from informal, non-institutional, online sources such as social media profiles to inform employment decisions. Ghoshray (2012) suggests that cybervetting includes gathering information from social media profiles without the job candidates' consent.

Given that cybervetting is informal and often relies on gathering information without asking the candidate first, it contrasts with traditional selection tools (Ghoshray, 2012; Berkelaar, 2008). Traditionally, the selection process consists of multiple formal steps, which typically begins with screening applications and resumes in order to find the best qualified person to perform a job (Noe, Hollenbeck, Gerhart, & Wright, 2011). After candidates submit a formal application for a position through submitting a resume or application, employers review the submissions to determine which candidates meet the basic qualifications for a job, such as required experience or skills to be able to successfully perform a job. Next, after narrowing down the selection pool for an open position, employers will test and review work samples (if applicable) and phone screen and interview candidates (Noe et al., 2011). The formal interview and testing process is designed to allow employers to compare applicants with each other and further narrow down the selection pool to a few qualified candidates. For these select candidates, employers will often check references provided by the job seekers and order formal

background checks to help inform their decision making process and ensure that the candidates will not pose any risk to the organization (Noe et al., 2011).

Instead of relying on a structured and formal selection process in which candidates consent to and often willingly provide much of the information considered such as resumes, applications, work samples, testing responses, interview responses, references, and lastly background check information, cybervetting searches and gathers information beyond that which is given willingly or intentionally from the candidate. According to Berkelaar (2008), the key difference between background checks (and arguably other traditional selection methods) compared to cybervetting “is the *access* (open vs. restricted) and the typical *nature* of information construction itself (informal and emergent vs. formal and intentional)” (p. 5). In regard to access and nature of information gathered for employment decisions, Berkelaar (2008) suggests that background checks, which require intentional consent on behalf of the applicant, are a much more formal process of acquiring information, as it includes services provided by government, financial, or other institutions that provide access to credit or other officially documented history that requires access privileges and/or payment. Similarly, one could argue that other traditional selection tools such as reviewing submitted resumes or applications, reviewing test results or work samples, and making decisions based on interview responses are also more formal and intentional methods in nature compared to cybervetting, as they rely on making decisions based on information that is willingly provided by the candidate and they are tools that can be equally used and compared among all applicants being considered for a position. Because cybervetting includes viewing candidates’ social media profiles, and not all applicants have social media

profiles or use it in the same way in regard to posting information or setting privacy settings, cybervetting is much more informal. Similarly, Van Iddekinge, Lanivich, Roth, and Junico (2013) found that although most recruiters indicated that they use SNS to make hiring decisions, they do not seek the same information for every applicant, making it especially difficult to use social media and other Internet information in a standardized way. In other words, while traditional selection methods aim to set all applicants on an equal playing field so candidates can be fairly compared and the most rational decision about who has the best skills and experience to perform the job can be chosen, cybervetting includes using different amounts of information that may or may not be available or reviewed for each candidate to make hiring decisions.

How Job Seekers Craft Their Online Identities

In order to investigate how the practice of cybervetting impacts job seekers' use of SNS, it is essential to understand how individuals create their identities on social media. According to boyd (2006), "SNS can be broadly defined as an Internet or mobile-based social space where people can connect, communicate, and create and share content with others" (p. 3). A unique characteristic of SNS is that it allows users the ability to build and represent their social identity online (boyd, 2006). SNS such as Facebook, LinkedIn, and Twitter are among the most popular, allowing people to connect with each other and share information and pictures (Moreau, 2016).

Although these SNS allow people to share information with others, these social media sites serve different purposes. For example, Facebook, a SNS that allows users to share their personal lives by posting photos and content, connecting with friends, and sharing information, is generally used for personal and social purposes (Pempek,

Yermolayeva, & Calvert, 2009; Van Dijck, 2013). Twitter, which is a microblog used to share short bursts of text, can serve multiple purposes, as it is normally utilized for both personal and professional purposes (Jin, 2013; Reinhardt, Ebner, Beham, & Costa, 2009). According to Reinhardt and colleagues (2009), 62% of the population surveyed use one Twitter account for both their professional and personal uses, while 23% strictly use it for professional communication, and only 15% use it for personal communication. LinkedIn, unlike Facebook, is usually used for professional purposes only (Van Dijck, 2013). Coined as the online resume (Schawbel, 2013), LinkedIn allows individuals to make career oriented connections with potential employers and other professionals, and it is usually utilized as an outlet for individuals to self-promote themselves and show off their professional experience (Van Dijck, 2013). Given that the three most popular social media websites are used for different personal or professional reasons, it is interesting to explore how individuals use these SNS to create their own identities.

With the emergence of technology and SNS, individuals are taking it upon themselves to create and manage their own online identities. SNS are popular tools for self-expression, communication, and self-promotion (Van Dijck, 2013). By posting their own content, editing their profiles and basic information, and selecting other members to connect with, people are crafting their identities and the way they are portrayed online. On social media, users are able to control what they post and whom they interact with, as well as establish numerous privacy settings. They have the ability to reveal as much (or as little) information about themselves through posting on their individual profiles (Bedijs, Held, & Maab, 2014). Beyond posting content, individuals can dictate what information outsiders have access to through privacy settings and accepting “friends” or

“followers,” allowing them to create and manage their identities for specific users to see. Since social media is a primary tool used for cybervetting (Ghoshray, 2012), it is important to understand the way individuals use SNS to create their identities.

One way that identity creation and maintenance on social media is understood is through the concept of facework. According to Floyd (2009), facework refers to the behavior people use to maintain their desired public image to others. On social media, people are believed to engage in facework, or acting in a way to ensure they are viewed positively by others (Bedijs et al., 2014; Imahori & Cupach, 2005). Given the ability to edit social media profiles and determine what content is posted and visible by specific people, individuals constantly manage their online identities so they appear positively, as facework suggests (Bedijs et al., 2014). By picking profile pictures and selecting the content that will be posted on social media, individuals are able to select how they portray themselves on each site in an effort to be seen positively, allowing them to control and manage their identities online.

Another way that identity creation and maintenance is understood is through the Communication Privacy Management Theory (CPM). According to CPM, individuals are selective in how they reveal and conceal private information to different people, which ultimately contributes to a person’s identity (Petronio & Durham, 2008). CPM suggests that all private information is owned by the person(s) who know(s) it (Petronio & Durham, 2008). When a person chooses to share the information, he or she is allowing someone else to be a co-owner of the information (Petronio & Durham, 2008). The information that people share with others normally depends on the boundaries that are in place, or the groups to which the potential receiver belongs to (Petronio & Durham,

2008). For example, when people are unfamiliar or new, a person may only reveal basic and non-intimate information, while concealing private information (Petronio & Durham, 2008). However, as the relationship with that person progresses, it is likely that more personal and private information will be shared in greater depth and breadth (Petronio & Durham, 2008). Jin (2013) found that on Twitter, users set multiple private disclosure boundaries, meaning that basic or non-intimate information is more likely to be disclosed, while private information is hidden from those who view the profile. According to CPM, these boundaries fall into three separate categories.

CPM is comprised of three components including boundary permeability rules, boundary ownership rules, and boundary linkage rules (Child et al., 2009; Child & Agyeman-Budu, 2010). Boundary permeability refers to the amount of breadth and depth a person chooses to disclose with others, while boundary ownership refers to the process of sharing information with another and allowing him or her to become a co-owner of the information (Child et al., 2009). Boundary linkage rules refers to the process of selecting who can receive certain information (Child et al., 2009). To measure these components in relation to an individuals' blogging activity, Child, Pearson, and Petronio (2009) developed survey items for participants to respond to with a Likert-type scale. This scale was later adapted to measure CPM in relation to users' Facebook activity by Frampton and Child (2013) and Child and Starcher (2016), who found evidence of users engaging in privacy management practices on Facebook.

In the context of social media profiles, individuals use CPM to determine what they share or conceal, which plays a part in their online identities. On SNS, people can determine who they connect with, manage their identities, and set a variety of privacy

settings similar to the methods of CPM, allowing them to select how they will be portrayed on social media. Research from Child, Petronio, Agyeman-Budu, and Westermann (2011) and Child, Haridakis, and Petronio (2012) discover that many users monitor their SNS and privacy settings often and even remove information that can be damaging. The degree of control varies for each social media type, but generally, social media settings can be configured to allow an individual to make their information public or private (boyd, 2006). For example, on Facebook, users are able to select friends, determine what information on their profile can be visible to the public or non-friends, and even create groups of people to give access to different information (Basic Privacy Settings & Tools, 2015). According to DiMicco and Millen (2007), users of SNS manage their identities through multiple user profiles and privacy controls, which allow them to conceal parts of their identities and keep their personal and professional lives on social media separate. Through the use of permissions and privacy settings, social media users can manage a variety of relationships online, as well as control their online presence, or how they are perceived by their close friends, family, acquaintances, or the general public (boyd, 2006). Similar to Facebook, individuals who use Twitter can also manage their identities through revealing their tweets to those they choose. For example, Twitter gives users the ability to set their tweets as public or private (Twitter Help Center, 2015). When a Twitter profile is set to private, the user must approve any followers, or people to connect with (Twitter Help Center, 2015). Once approved, the followers are able to view the user's Twitter profile and any tweets published (Twitter Help Center, 2015). Through privacy settings across popular social media platforms like Twitter and Facebook, social

media users are able to craft their identities by choosing who they reveal or do not reveal certain information to, as characterized by CPM.

When it comes to crafting and managing identities on social media, both CPM and facework present a valuable understanding that is helpful in making sense of how social media behavior and self-disclosure affects online identity. The concept of facework focuses on what an individual strategically reveals on SNS to make him or herself appear positively, while CPM, though mentioning how an individual strategically discloses information on social media, emphasizes the information that individuals strategically choose not to reveal. These two concepts promote the idea that an individuals' online identities are made up of what they choose to reveal or conceal about themselves. By understanding how individuals use facework and CPM to strategically reveal or conceal information to craft their online identities, the effect of cybervetting on identity creation and social media use can be better understood. However, it is also essential to understand how pervasive cybervetting is and why employers use it.

How Organizations Use Cybervetting

Because so many individuals have a presence on social media, organizations are taking advantage of the available information to uncover information about job candidates (Davison, Maraist, Hamilton & Bing, 2012; Ghoshray, 2012). Ghoshray (2012) notes that some employers are even considering cybervetting a key selection process when finding candidates to fill a position.

In recent years, organizations' use of cybervetting job applicants has increased tremendously. The Ponemon Institute (2007), for instance, found that 35% of hiring managers use the search engine Google to conduct background searches, which can lead

to cybervetting of candidates' SNS that are connected with their names when searched. Petriches, Fuller, Marciw, and Conquest (2015) even consider online searching and cybervetting to be the new hiring background check. Additional research from Levinson (2010) finds that over 73% of the roughly 860 surveyed human resources managers either use or plan to use SNS in some part of the hiring process when deciding between job candidates, while 30% of these respondents revealed that they always check social media profiles when making hiring decisions. Furthermore, a CareerBuilder survey indicated that 37% of over 2,300 hiring managers look up candidates on social media to gather information, and even more plan to start using these tools in the future (Grasz, 2012). In addition, nearly 30% of hiring managers indicated that they had not hired applicants due to what they saw on applicants' SNS (Van Iddenkinge et al., 2013).

Given the popularity of cybervetting to screen job applicants, it is interesting to explore why organizations cybervet. Research shows that organizations cybervet job applicants for three main reasons. The first reason an organization cybervets is because it is a cheap and convenient way to gather information about individuals (Petriches et al., 2015; Van Iddenkinge et al., 2013; Clark & Roberts, 2010; Levashina & Campion, 2009). According to Clark and Roberts (2010), SNS are "serving as an inexpensive and quick source of background information" on job applicants (p. 507). Because employers can find information about a job candidate by going on Google and searching for names and social networking profiles, they see cybervetting as a way to gather information, while not spending any money (Petriches et al., 2015). SNS are considered to be cheap and convenient because the information already exists and is available (i.e., it does not have to be developed or created), it is essentially free to view, and it does not require

applicants to be physically present (Van Iddenkinge et al., 2013). Similarly, Levashina and Campion (2009) suggest that cybervetting is becoming widely adopted among organizations because the Internet and SNS are convenient and inexpensive ways to screen candidates to ensure they meet minimal professional standards, are competent to do their job, and do not pose a foreseeable danger to the organization. Because so many people are on social media and they are constantly updating their profiles, individuals' personal information is easily accessible for organizations to consider during the hiring process.

Another reason that organizations use cybervetting is to find out more information about candidates, beyond what their resumes display (Petriches et al., 2015, Berkelaar, 2014; Davison, Maraist, & Bing, 2011). According to Berkelaar (2014), resumes provided by applicants are becoming increasingly hard to trust. Because employers are worried about deception and extreme impression management on behalf of job applicants, they are questioning the accuracy of resumes, and are instead looking to social media profiles to provide more information (Berkelaar, 2014; Barrick, Shaffer, & DeGrassi, 2009; Griffith & Converse, 2011).

Specifically, employers are looking to job applicants' social media profiles to gauge their personalities and determine if they would be a good fit for the organization. Because personality is often hard to determine with a resume, organizations are looking to applicants' social media profiles to uncover what kind of person they are (Petriches et al., 2015; Berger & Douglas, 1981). In other words, because cybervetting reveals information usually communicated for purposes other than career advancement, it can be viewed as providing access to a person's true self (Berger & Douglas, 1981). For

example, an employer quoted in *HR Magazine* stated that “there is nothing that screams more accurately who you are than a Facebook page” (Mienert, 2011, p. 31). Results from a CareerBuilder survey indicate that employers use social media to determine whether a candidate would fit well in an organization (Grasz, 2012). When it comes to employers considering the information they find on a candidate’s social media, including public posts and pictures, they often view social media as more accurate than a cover letter, resume, or interview because it is considered to be more of a true representation of a person’s personality (Davison et al., 2011). However, it is important to note that although social media can reveal some insight into a person’s personality, there is conflicting research on whether or not SNS are an accurate depiction of a person’s identity and personality, which is mainly due to the individual’s ability to craft his or her online identity through CPM and facework tactics described previously.

The third reason employers use cybervetting is to avoid risk and maintain their company’s positive reputation (Shilling, 2009; Haefner, 2009; Clark & Roberts, 2010; Anthony, Perrew, & Kacmar, 1999; Ghoshray, 2012). If an employer does not perform a thorough background check on a hired employee and the employee inflicts harm on a customer or a third party that could have been predicted by the employer, the organization can be found guilty of negligent hiring (Shilling, 2009; Anthony et al., 1999). The emergence of the Internet and the accessibility of information has resulted in an increased expectation that organizations will thoroughly vet job candidates and conduct background checks (Levashina & Campion, 2009).

To avoid hiring employees who could potentially damage the reputation of the organization, Haefner (2009) reveals that many hiring managers are using SNS to screen

out applicants. According to Haefner (2009), if a job applicant posts pictures of behaviors on social media that are considered to be inappropriate for the workplace, such as excessive drinking, partying, drug use, and/or violent behavior, he or she is likely to be withdrawn from consideration for a position. Davison and colleagues (2011) found that a qualified college student who applied for a summer job as a camp counselor was eventually denied the position because the organization had seen pictures on her social media profile depicting her engaging in binge drinking. This job applicant is not alone, as organizations report that they have eliminated candidates from the selection process if they are found to be posting things on social media that could ultimately reflect badly on the organization's reputation (Clark & Roberts, 2010; Davison et al., 2001; Haefner, 2009; Shilling, 2009).

Consequences of Cybervetting

Given that cybervetting is becoming a popular tool to inform hiring decisions, it is imperative to explore the implications and issues of this practice. According to Van Iddekinge et al. (2013), Levinson (2010), SHRM (2008), Davison et al. (2011), and Brown and Vaughn (2011), there are some issues with using cybervetting as a method to make hiring decisions. One implication of using cybervetting is that it can lead to making decisions based on inaccurate information or information that may not be applicable to active performance on the job (Davison et al., 2012; Brown & Vaughn, 2011). Van Iddekinge and colleagues (2013) state that SNS may not provide job-related information because they are designed for social interaction rather than for hiring or personnel selection. Additionally, Van Iddekinge and colleagues (2013) suggest that it is still unclear whether using social media profiles to make hiring decisions is considered valid

and legally defensible under the law, especially since the *Uniform Guidelines* (Equal Employment Opportunity Commission [EEOC], 1978) state that selection procedures should test criterion related to the job. For example, Haefner (2009) reports that 35% of hiring managers have found reasons to not offer candidates a job because of information displayed on online social networks. Since social media profiles may not be true depictions of how well a candidate could perform a job, these employers may have misjudged and passed up great applicants. By conducting a study with job seekers and recruiters, Van Iddenkinge and colleagues (2013) found that there is no correlation between the comparison of recruiters' ratings of job seekers' Facebook profiles and their actual performance in the job, meaning that "these organizations appear to be assessing SM (social media) information in the absence of data concerning the validity of inferences made on the basis of such information" (p. 16). Because organizations who use cybervetting are using it to making hiring decisions despite having no evidence of a candidate's social media profile being any indication of how that individual would actually perform on the job, the use of social media information to make selection decisions can be considered inappropriate (Van Iddenkinge et al., 2013).

One reason that SNS may not be a good indicator of how successful a person could be in a position is that negative information or impressions conveyed through an applicant's personal profile might not be considered in the proper context, and therefore, could result in an irrational rejection decision (Brown & Vaughn, 2011). As a result, acting solely on the information obtained from SNS to make employment decisions without validation or verification from other sources can lead to potentially great candidates being eliminated from the hiring process (Davison et al., 2011).

Another consequence of using cybervetting is that it can potentially contribute to illegal discrimination of applicants in the hiring process (Brown & Vaughn, 2011; Davison et al., 2012; Abril et al., 2012; Kluemper, 2013; Van Iddenkinge et al., 2013). Brown and Vaughn (2011) argue that employers may be at risk of providing preferential consideration early in the hiring process by using social media profiles to make decisions. A wide range of demographic information is easily available to decision makers who choose to review job candidates' SNS (Van Iddenkinge et al., 2013). According to the United States Equal Employment Opportunity Commission (EEOC), a variety of different classes are protected against hiring and employment discrimination, including characteristics such as age, disability status, sex, religion, national origin, race, and pregnancy. Because such information is prohibited by the EEOC from being used in the decision making process and it can potentially be accessed through information and pictures posted on SNS, organizations may fall into the trap of using this information to make selection decisions. To this point, Acquisti and Fong (2013) discover that employers are more likely to seek candidates who are a closer ethnic match to themselves or other employees at the organization, meaning that candidates may be eliminated from consideration based on their ethnicity. More specifically, the study found that Muslim candidates are less likely to be offered a job compared to Christian candidates (Acquisti & Fong, 2013). Since this information is readily available on SNS, it may ultimately lead to discrimination in hiring decisions. In these cases, the burden of proof may fall on the organization to demonstrate that protected groups, as designated by the EEOC, did not impact the hiring decision (Van Iddenkinge, 2013). According to Mander (2012),

because of the possibility of discrimination or making decisions based on things that are unrelated to the job, many people feel that cybervetting using SNS is unfair.

In addition to the possibility that cybervetting can lead to discrimination in the hiring process, another consequence of cybervetting is that it can be viewed as an invasion of privacy, and may, in fact, influence the way in which employees portray themselves online (Abril et al., 2012; Brandenburg, 2007). Because employers are using SNS to gain information for hiring decisions, some applicants feel as though their freedom of speech and right to privacy are being violated, as their personal social media accounts that display their self-created identities are being judged by employers (Brandenburg, 2007; Abril et al., 2012). According to Abril and colleagues (2012), “private information that was previously segregated now becomes easily accessible to employers, colleagues, recruiters, and clients, among other perhaps unintended audiences,” which has consequences for individuals’ personal privacy and self-expression of identity on social media (p. 64). Furthermore, Berkelaar (2010) and Ghoshray (2012) also suggest that cybervetting typically occurs without job applicants’ permission or opportunity for correction, which amplifies the invasion of privacy. Currently, employers have few policies in place to govern and dictate how and when SNS should be used and how to ensure the information obtained is accurate (Clark & Roberts, 2010). While student privacy (FERPA) and medical privacy (HIPPA) have been addressed in the law, personal privacy in regards to cybervetting using SNS has yet to be examined in detail. This is a potential issue that both organizations and job applicants should be aware of now and in the future, especially as cybervetting becomes more popular.

Even though job seekers are not informed that their social media profiles will be a deciding factor in an organization's hiring process, many have started to anticipate that their social media profiles will be examined upon being considered for a position, which leads to their likelihood of modifying their online identities to impress employers (Clark & Roberts, 2010).

Given that job applicants are starting to realize that their SNS may be viewed by a potential employer, this study proposes the following research questions:

RQ 1: How does cybervetting impact job seekers' social media use?

RQ 2: How does cybervetting impact job seekers' online identity creation on social media?

These two research questions, while separate, are interrelated in terms of how identity is created, managed, and observed in social media. Given the nature of social media, use of social media or behavior on SNS directly influences an individual's online identity on social media, and vice versa. Essentially, social media use and SNS identity creation is a simultaneous process, because when individuals use social media, they are crafting their online identities, and when individuals look to craft their identities on SNS, they use social media in a specific way.

Using the frameworks of CPM and facework, this study explores how job seekers are using social media, privacy settings, and revealing or concealing information in reaction to organizational cybervetting. Facework encompasses what individuals actively put forward or reveal on SNS in order to appear positively for others, while CPM emphasizes what individuals strategically hold back from others, both of which contribute to individuals' online identities. This study specifically focuses on the social

media sites of Twitter and Facebook, as they are SNS that are used for personal and social purposes.

Chapter Three: Methodology

This study seeks to answer the research questions through a series of measures examining social media use, privacy management, privacy tools usage, and overall concern for cybervetting. Some basic demographic items were included in the survey to gather information about the sample, including employment or job seeking status, age, gender, major, and whether the individual used social media. Only participants who indicated that they used social media in the introductory demographic section of the survey were accepted to participate. (See Appendix A for scales and questions.)

Participants and Procedures

In order to gain information about how the use of cybervetting influences job seekers' use of social media, specifically on Twitter and Facebook, this study used online surveys to gather quantitative data through the use of Likert-scale type items and qualitative data through the use of open-ended questions. Online surveys were distributed to seniors at a private Midwest university, who are presumably current job seekers, or are likely to be in that position soon. A random list of potential participants, who met the senior status criteria, was provided by the university.

For this study, 56 people responded to the online survey. Out of the respondents, 51 participants were included in the data analyses, which consisted of 15 males (29.4%) and 36 females (70.6%). A total of five participants were omitted from data analyses due to two participants not using social media, which was a requirement for the study, and three other participants not completing the entire survey. Of the data that was included in the analyses, respondents' ages were between 21-31 ($M = 21.49$, $SD = 1.72$), and 82.4% of participants were White, 3.9% of participants were Black or African American, and

13.7% considered themselves as “other.” For employment status, 31.4% of participants were not actively job seeking but will in the next six months, 33.3% were passively seeking, 15.7% were actively seeking, 13.7% were offered and have accepted a post-college position, and 5.9% were not seeking and unemployed. (See Table 1 for all participant demographics.)

Table 1: Participant Demographics

Age, <i>M (SD)</i>	21.49	(1.72)
Gender, <i>n (%)</i>		
Female	36	(70.6)
Male	15	(29.4)
Ethnicity, <i>n (%)</i>		
White	42	(82.4)
African American	2	(3.9)
American Indian or Alaska Native	0	(0.0)
Hispanic or Latino	0	(0.0)
Asian or Pacific Islander	0	(0.0)
Other	7	(13.7)
Employment Status, <i>n (%)</i>		
Not seeking and unemployed	3	(5.9)
Not seeking yet, but will in 6 months	16	(31.4)
Passively job seeking	17	(33.3)
Actively job seeking	8	(15.7)
Offered and accepted post-college position	7	(13.7)
Social Media Use, <i>n (%)</i>		
Social Media User	51	(100)
Facebook User	28	(54.9)
Twitter User	15	(29.4)
Instagram User	21	(41.2)
LinkedIn User	17	(33.3)
Snapchat User	23	(45.1)

N = 51

Since social media use was a prerequisite for the study, all participants involved in data analysis (*n* = 51) were social media users. Of the respondents, 100% use Facebook, 53.6% use Twitter, 70.4% use Instagram, 60.7% use LinkedIn, and 77.8% use

Snapchat, with participants having an average friend and/or follower base of 849 people. According to the responses to the Social Media Intensity Scale, participants spend 4.68 hours on average per day on social media ($SD = 2.24$), and a total of 86.3% of participants indicated that they either “somewhat agree” or “strongly agree” that social media is a part of his or her daily routine.

Measures

Social Media Intensity Scale.

Since this study explores how cybervetting influences job seekers’ social media use and online identity creation, it is important to gain an understanding of how often participants use social media. Following suit of Ellison, Steinfield, and Lampe (2007), this study incorporated a Social Media Intensity Scale. Ellison et al.’s (2007) scale was originally designed to measure Facebook, but it was adapted in this study to include Twitter in addition to Facebook since Twitter also includes some degree of personal identity creation and connecting with others. Additionally, Twitter and Facebook have similar features, with users being able to allow people to follow or friend them, post text and pictures, and interact with others in a personal way. The measure has two assessments of behavior regarding social media, both designed to measure the extent to which the participant actively engages in social media activities, including the number of “friends” and the daily amount of time spent on social media. The measure also includes Likert-scale type items designed to measure the extent to which a participant is emotionally connected to some form of social media (Ellison et al., 2007). For the current study, this measure yields a Cronbach’s alpha score of .88, which indicates that there is internal consistency between the items in the scale.

CPM Social Media Scale.

This scale, which originally was designed to measure privacy management (CPM) with blogging, was adapted in this study to measure privacy management on social media, similar to the Frampton and Child (2013) and Child and Starcher (2016) studies that adapted the scale to Facebook. This scale includes 18 statements, where participants responded with a seven point Likert scale ranging from strongly disagree to strongly agree. The scale has three dimensions, which are designed to measure different components of privacy management (Child et al., 2009). This CPM scale is useful for this study because it can help connect CPM to the study and help determine, through data analysis, if a relationship exists between privacy management and concern for cybervetting. Ultimately, this scale helps provide insight about how job seekers' social media use and online identity creation may be influenced by organizations' use of cybervetting.

The first dimension in this scale measures the privacy boundary permeability process. Higher scores indicate that the permeability rules operated in a more public manner, where there is a higher level of breadth and depth of disclosure on social media (Child & Agyeman-Budu, 2010; Child et al., 2009). In this study, the Cronbach's alpha score for Boundary Permeability is .79, meaning that there is internal consistency between the items in the scale. Child and Agyeman-Budu (2010), who used the CPM scale in their study, also had a high reliability score ($\alpha = .76$) for Boundary Permeability.

The second dimension of this scale measures the privacy boundary ownership process. Higher scores suggest that a participant freely shares the rights and privileges for information disclosed on their SNS, and he or she is less concerned about who is seeing

and reading the information posted (Child & Agyeman-Budu, 2010; Child et al., 2009). In this current study, the Cronbach's alpha score for the Boundary Ownership is .58, indicating that there is low internal consistency between the items in the scale. This finding is much lower than what Agyeman-Budu (2010) found in their study regarding the reliability for Boundary Ownership ($\alpha = .70$).

The last dimension in this scale measures the privacy boundary linkage process. Higher scores mean that a participant expends more conscious effort in determining who has access to his or her SNS (Child & Agyeman-Budu, 2010; Child et al., 2009). For Boundary Linkages, this current study yields a Cronbach's alpha score of .84, indicating that there is internal consistency between the items in the scale. This finding is similar to what Child and Agyeman-Budu (2010) found in their study regarding the reliability for Boundary Linkages ($\alpha = .71$).

Similar to the Social Media Intensity Scale, the CPM Social Media Scale also only gathers data regarding participants' Facebook and Twitter uses, as they are social media that can be used for personal and social uses.

Technological Privacy Tools Measure.

Following suit of Litt (2013), this study also utilizes the Technological Privacy Tools Measure to gain information about how job seekers change their privacy settings. "This variable is composed of an index that sums the number of technological privacy tools an individual reported using. This index is composed of responses (yes = 1, no = 0) to a set of five questions" (Litt, 2013, p. 1652). This variable is compared with the Concern for Cybervetting Measure to explore whether there is a relationship between the participants' concern for cybervetting and their action to protect their social media

profiles. Similar to the above measures, this measure only prompted users to think specifically about their Twitter and Facebook use.

Concern for Cybervetting Measure.

In order to measure how concerned participants are with cybervetting in regards to their social media profiles, a nine-item measure was created to gauge their concern. This scale prompted individuals to respond with a five point Likert-type scale, ranging from strongly disagree (1) to strongly agree (5) for five statements. The remaining six statements included open-ended follow-up questions for some of the statements to gather qualitative data about participants' responses. The items in this scale were strategically worded to not mention or refer to cybervetting or potential employers in any way to prevent participants from being primed to think about cybervetting. The goal of this measure is to obtain honest opinions about if participants think about employers or potential employers looking at their social media pages to make hiring decisions. Similar to the other scales, this measure only examined participants Twitter and Facebook social media use. For the results, this scale is compared with the Technological Privacy Tools Measure and the CPM Social Media Scale to determine if a relationship exists between concern for cybervetting and actions taken to maintain social media privacy and protection. The current results indicate that there is a low Cronbach's alpha for this measure ($\alpha = .55$), which means that there is not strong internal consistency among the items, most likely due to the small number of items and small number of participants.

Chapter Four: Results

After the survey data was collected from participants, the Likert scale responses from the Social Media Intensity Scale, CPM Social Media Scale, Technological Privacy Tools Measure, and the Concern for Cybervetting Scale were analyzed through the use of statistical methods, including calculating averages, running reliability tests, and correlations to determine what relationships exist between the key variables. The open-ended responses were analyzed through an independent thematic analysis, where each response was assigned a rating and common themes were identified among the responses. Paired with the statistical analysis, the thematic analysis provided additional insight into the relationships between key variables. The results are provided below.

The online survey, which had a total of 51 participants, utilizes different Likert scale-based measures. The first scale in the study is the Social Media Intensity Scale, which yields a mean of 3.70 ($SD = .88$) for its six Likert scale items. The CPM Social Media Scale, which has three components with six corresponding statements each, yields an overall mean of 4.53 ($SD = .46, n = 49$). When looked at individually, the first component, Boundary Permeability, has a mean of 5.98 ($SD = .89, n = 50$), while the second component, Boundary Ownership, has a mean of 4.98 ($SD = .76, n = 50$). The last component, Boundary Linkages, yields a mean of 2.70 ($SD = 1.12, n = 49$). The Technological Privacy Tools Measure yields a mean of 4.17 ($SD = .95$). The final scale that uses Likert scale statements is the Concern for Cybervetting Measure, which has a mean of 3.85 ($SD = .73, n = 48$).

Aside from collecting demographic information from the participants, the quantitative analyses for this study consisted of examining correlations between the

Concern for Cybervetting Measure, Social Media Intensity Scale, the CPM Social Media Scale and components, and the Technological Privacy Tool Measure. (See Table 2 for all primary correlations.)

Table 2: Correlations Between Key Variables

($N = 51$)

Concern for Cybervetting (CFC), Boundary Permeability (BP), Boundary Ownership (BO), Boundary Linkages (BL), CPM Components (CPM), Social Media Intensity (SMI)

	CFC	BP	BO	BL	CPM	SMI
1. CFC	1	-.009	.089	-.048	.003	.332*
2. BP	-.009	1	.359*	-.473**	.445**	-.409**
3. BO	.089	.359*	1	-.119	.664**	-.289*
4. BL	-.048	-.473**	-.119	1	.440**	.225
5. CPM	.003	.445**	.664**	.440**	1	-.247
6. SMI	.332*	-.409**	-.289*	.225	-.247	1

* $p < .05$ ** $p < .01$

The relationship between the Concern for Cybervetting Measure and the Social Media Intensity Scale was explored using correlations. The results show that there is a statistically significant positive correlation present between the two scales ($r = .359$, $p < .05$), indicating that participants who use social media more express a greater concern for cybervetting.

Before examining the relationships between the CPM Social Media Scale and the other scales, the relationship between each of the CPM scale components and the overall scale were analyzed first. The results show that there is a statistically significant correlation present between Boundary Permeability and the other components of

Boundary Ownership and Boundary Linkages, and each of the components are statistically significantly correlated with the overall CPM scale.

According to the results, the first component, Boundary Permeability, has a statistically significant correlation with Boundary Ownership ($r = .359, p < .01$), and Boundary Permeability has a statistically significant correlation with Boundary Linkages ($r = -.473, p < .01$). The Boundary Permeability component also has a statistically significant correlation with the overall CPM Social Media Scale ($r = .445, p < .01$). The results also show that Boundary Permeability has a statistically significant correlation with the Social Media Intensity Scale ($r = -.409, p < .05$). This negative correlation indicates that the more participants use social media, the less likely they are to share personal information, create detailed posts, and discuss work concerns, as characterized by the behaviors that align with the Communication Privacy Management Theory of Boundary Permeability.

The second component, Boundary Ownership, has a statistically significant correlation with the overall CPM scale ($r = .664, p < .01$). The results also show that Boundary Ownership has a statistically significant correlation with the Social Media Intensity Scale ($r = -.289, p < .01$). This negative correlation indicates that the more participants use social media, the less likely they are to share private information and topics, as characterized by the behaviors that align with the Communication Privacy Management Theory of Boundary Ownership.

Furthermore, the third component, Boundary Linkages, has a statistically significant correlation with the overall CPM scale ($r = .440, p < .01$). Overall, these

statistically significant correlations between the components indicate that there is a relationship between the overall CPM scale.

After examining the relationship between the overall CPM scale and the Concern for Cybervetting Measure, the results indicate that there is no statistically significant correlation between the two measures. The relationship between the Concern for Cybervetting Measure and the Technological Privacy Tools Measure was also analyzed and revealed no statistically significant results.

The qualitative analyses for this study consisted of an independent thematic analysis of the open-ended responses collected on the online survey. Through the use of a thematic analysis following the guidelines provided by Braun and Clarke (2006), common themes among the participants' responses were identified first. The thematic analysis was approached inductively, in that the themes and coding development was directed by the content of the responses. Code categories were identified for each open-ended question, and each response was considered on an individual basis and labeled with a code number most similar to one of the coding categories. The responses to each question typically fell into one category, with some responses falling into more than one. Information about the coding categories and codes assigned to each response can be found in Appendices B-F.

For open-ended items that asked participants to elaborate on who they would be hesitant to connect with on social media and why, the results of the coding reveal that 86% of participants indicated that they are hesitant to connect with people who are strangers or that they do not know, with a couple of participants indicating that they were concerned with employers or potential employers. In addition, 23% of participants

directly indicated that they were hesitant to connect with either employers or people they do not know because they were concerned with providing them access to their personal information displayed on social media. According to one participant, he or she is hesitant to connect with an employer because that individual has a desire to “keep social and professional lives separate.” These results indicate that the majority of participants desire to keep their social media connections to only people they know, and some are hesitant to make any employer or job-related connections on social media.

For the open-ended question examining how the audience impacts the social media content that they produced, the results indicate that 27% of participants mentioned that they control what they post on social media because an employer, potential employer, and/or co-worker might see their information. A couple of participants directly expressed a concern for cybervetting when one states, “Since I know that potential employers as well as my parents and their friends are looking at my social media pages, I would not post anything with offensive language, and I definitely don't share the kind of personal details I would share with a close friend,” and another states “I don't want the adults/future employers seeing inappropriate pictures (posted on social media).” Additionally, 23% of participants indicated that they are concerned with posting offensive content or content that audience members of their social media profile pages may not approve of, with 18% of participants specifically mentioning how family impacts what they post on social media. Twenty-three percent of participants also indicate that they cater their social media posts to what people want to hear.

Additionally, the survey prompted participants to indicate whether they are concerned about how organizations that he or she may have a relationship with perceive

their social media profile(s). If participants had a concern, they were asked to indicate what they were concerned about. The results show that 50% of participants directly mention or refer to their ability to be hired or their professionalism. Furthermore, 36% of participants directly mention their concern to not post inappropriate or offensive information. One participant expressed, “I am nervous about not getting a job due to social media so I try to be thoughtful through my posts,” while another stated the he or she is concerned with “Maintaining a somewhat professional profile on Facebook so that future employers may not be driven away from what could be a harmful post.” Another participant expressed concern for cybervetting by saying, “I want to stay respectful online and offline. I want my employers to search me and not be turned off by what they see (even if they can’t see anything due to privacy settings) and I am friends with my family members so I wouldn’t want to post anything I wouldn’t feel comfortable talking to them about,” and another participant states, “. . .I am also concerned for my future employment and my social media must reflect the professional person that I am.” These results affirm that individuals have a concern for cybervetting as it relates to how they use their social media and display themselves online.

Finally, participants were asked a follow-up question about when their concern originated. The data revealed that 36% of participants directly refer to this concern beginning due to job-seeking or learning that employers may use information from their social media profiles to make hiring decisions. Another 36% identify college or high-school as the time that their concern for what they post on social-media originated, with 14% of participants suggesting that their concern has always been present. Two participants describe their concern for potential employers using social media to make

hiring decisions when they state, “When I started looking for jobs in high school, some people told me that job recruiters may look at potential employees' social media,” and “Upon learning that employers can check Facebook profiles while looking for job candidates.” Furthermore, another participant indicated that his or her concern began with “...hearing discussions about organizations using social media profiles to gather information on people, especially potential employees.” Other participants stated that “When I started looking for jobs,” “Job seeking,” and “Entering college and considering applying for jobs” started their concern for what they post online.

Chapter Five: Discussion

Although cybervetting can be a convenient and efficient way to help reveal a candidate's personality and eliminate risk to an employer, there can be a variety of consequences, some of which have not been thoroughly explored in the research to date. Accordingly, this study examines how cybervetting may pressure job seekers to change their online identities to impress potential employers. Through using the Social Media Intensity Scale, the CPM Social Media Scale, the Technological Privacy Tools Measure, and the Concern for Cybervetting Measure, this study explores job seekers' social media use and identity creation in light of the prevalence of cybervetting.

To answer the first research question of "How does cybervetting impact job seekers' social media use?," the results indicate that participants are using a variety of privacy tools on SNS, and participants refer to some sort of concern for cybervetting. The results also show a direct positive relationship between the social media use and concern of cybervetting, with those who use social media more expressing a greater concern for cybervetting. To answer the research question of "How does cybervetting impact job seekers' online identity creation on social media?," the results suggest that individuals are expressing a concern for cybervetting and are choosing what to share and conceal through the use of privacy settings, facework and CPM behaviors, which plays a part in their identity creation on SNS. These conclusions were reached by comparing the scales to previous studies, testing the reliability for each scale, running correlations between all key variables, and conducting an independent thematic analysis of the responses to the open-ended questions.

When examining the values of the Social Media Intensity Scale in the present study, it is apparent that the mean for the Likert scale statements are similar to Ellison et al.'s (2007) study, with the current study yielding a mean of 3.70 and Ellison et al.'s (2007) study yielding a mean of 3.06. Although Ellison et al.'s (2007) scale has a mean that is slightly lower than the current study, it is likely reflective of the increase in social media, particularly on Facebook and Twitter in the last decade. According to the Pew Research Center, 90% of young adults use social media, which is much higher than the 12% that were reported in 2005 (Perrin, 2015). This increase in social media use, especially among the sample, which were young adults in this current study, likely led to the higher mean (or more social media use) reflected in the Social Media Intensity Scale.

When comparing the values of the CPM Social Media Scale in the present study to Child et al.'s (2009) study, both differences and similarities were identified. In Child et al.'s (2009) study, which used the CPM scale in regard to blogging, the results yield a much lower mean for Boundary Permeability ($M = 2.81$) and Boundary Ownership ($M = 3.36$) than the current study, which yields a mean of 5.98 and 4.98 respectively. However, Child et al.'s (2009) study yields a similar, but slightly higher mean for Boundary Linkages ($M = 3.01$) compared to the present study, which yields a mean of 2.70. These differences and similarities can be attributed to the similarities and differences between blogging and social media, as both are similar in the sense that they include self-disclosure, but are different in how SNS typically facilitate more communication between individuals than blogging, which may promote individuals to share even more personal information on social media that aligns with the CPM statements in the survey.

When comparing the values of the Technological Privacy Tools Measure in the current study to Litt's (2013) study, it is apparent that the privacy tools are more frequently used by the current study's sample. Litt (2013) found that, on average, participants used a little less than two and a half of the privacy tools, while participants in the current study report, on average, engaging in at least four of the five privacy tools ($M = 4.17$). Additionally, the results of the current study indicate that all of the participants used at least two or more privacy tools on social media, while Litt (2013) found that more than 16% did not use any privacy tools and roughly 16% only used one tool. Furthermore, similar to Litt (2013), the most frequently used privacy tool is adjusting one's privacy settings, with 100% of participants in current study compared to 65% in Litt's (2013) study reported to have changed their social media privacy settings. Considering that the current study is examining job seekers, the increase in the use of privacy settings may be due to the participants' concern for organizations' cybervetting, as indicated by the direct mention of cybervetting-like behaviors found in the thematic analysis. Furthermore, as Litt (2013) indicates, younger adults, which make up the current study's sample, are more likely to utilize technological privacy tools than older adults. Because the current study only incorporated participants who are younger adults, it is fair to link the higher usage of privacy tools on social media to the higher number of younger adults in the sample.

The last scale, which is the Concern for Cybervetting Measure, cannot be easily compared to previous studies because it is a brand new measure developed specifically for this study. Because the measure is new and there were a limited number of participants in the study, the Likert scale statements yield a low reliability, making it

difficult to get a true and generalizable understanding of cybervetting concern among job seekers. Although there is low-reliability associated with the Likert scale items, the responses to the open-ended questions in this measure do a great job of not only explaining the cybervetting concern, but also the nature of this concern.

In order to address the research questions of “How does cybervetting impact job seekers’ social media use?” and “How does cybervetting impact job seekers’ online identity creation on social media?,” this study specifically examines whether relationships exist between the key variables, including the Social Media Intensity Scale, the CPM Social Media Scale, the Technological Privacy Tools Measure, and the Concern for Cybervetting Measure.

When a correlation examining the relationship between social media use (Social Media Intensity Scale) and Concern for Cybervetting was conducted, the results indicate that there is a statistically significant positive correlation, suggesting that participants who use social media more express a greater concern for cybervetting. According to these results, the more participants indicated that they use Facebook and/or Twitter, the more concern they have for potential employers engaging in cybervetting behaviors. Essentially, this finding promotes the idea that social media users, such as job seekers in the case of this study, are expressing some sort of concern for cybervetting, which may suggest some type of impact on their social media identity creation and behavior. However, because the Concern for Cybervetting Measure had low reliability, it is hard to confidently say whether or not this relationship exists based on this correlation. However, given that all participants in the study use social media and many alluded to some type of concern for cybervetting in the open-ended responses, it is likely that the more time

participants spend on social media, the more they may be concerned about potential employers finding information on their SNS that can negatively impact hiring.

Another correlation ran between the Social Media Intensity Scale and a component of the CPM Social Media Scale, Boundary Permeability, also indicates that there is a negative relationship between social media use and Boundary Permeability. This negative correlation suggests that the more participants use social media, the less likely they are to share personal information, create detailed posts, and discuss work concerns, which align with the CPM Theory of Boundary Permeability. The results also indicate a significant negative correlation with the Social Media Intensity Scale and another component of CPM, Boundary Ownership. This negative correlation suggests that the more participants use social media, the less likely they are to share private information and topics, as characterized by the behaviors that align with the Communication Privacy Management Theory of Boundary Ownership.

Going along with the concern for cybervetting ideal, participants, especially job seekers in the case of this study, are more likely to refrain from posting personal information, private information, and/or about work concerns because it may negatively impact the likelihood of being chosen for a position. Results from the independent thematic analysis support these ideas, with 50% of participants indicating a concern for professionalism in regard to their social media use influencing a relationship with an organization. When asked about what he or she is concerned about when posting on social media, one participant expressed that he or she is concerned with “How the organizations view me.” Another participant states, “...I am also concerned for my future employment and my social media must reflect the professional person that I am,” and

another said “I am concerned about how appropriate my posts may be to outsiders and professional connections.” In some cases, oversharing personal information or posting about work concerns can be considered unprofessional, so it makes sense that the more participants use social media, the more likely they are to be cognizant of how oversharing personal or private information or complaining about work can reflect negatively upon them.

Examining the relationship between the Concern for Cybervetting Measure with the overall CPM Social Media Scale and the Technological Privacy Tools Measure, the results indicate that there are no statistically significant correlations. These findings are likely due to the small amount of items, small number of participants, and the low Cronbach alpha in the Concern for Cybervetting Measure. Because of the low reliability for the Concern for Cybervetting Measure, it is hard to confidently explain the relationship between that and the CPM Social Media Scale and the Technological Privacy Tools Measure.

Although there were no statistically significant results found between the Concern for Cybervetting Measure and the CPM Social Media Scale and the Technological Privacy Tools Measure and no relationship can be confidently identified, the thematic analysis of the open-ended responses suggests that participants have a concern for cybervetting that is related to their social media use. Specifically, 27% of participants stated that they monitor what they post on SNS because an employer, potential employer, and/or co-worker may view the information. One person even mentioned, “Since I know that potential employers as well as my parents and their friends are looking at my social media pages, I would not post anything with offensive language, and I definitely don't

share the kind of personal details I would share with a close friend,” while another person mentioned “I don't want the adults/future employers seeing inappropriate pictures (posted on social media).” According to these statements, some participants’ social media use is influenced by potential employers, which supports the idea that cybervetting impacts how they use social media and maintain their online identities. This idea is further supported with the findings around when participants’ concern for their social media content began. Thirty-six percent of participants directly mention job-seeking or learning that employers may use information from individuals’ social media profiles to make hiring decisions as the starting point for this concern. One participant discusses a concern about what they post on social media beginning, “Upon learning that employers can check Facebook profiles while looking for job candidates” and another participant stated that this concern began with “...hearing discussions about organizations using social media profiles to gather information on people, especially potential employees.” These results suggest that a number of participants are concerned with how their social media profiles can impact how potential employers view them. These findings from the thematic analysis, paired with the strong usage of privacy settings and tools as indicated by the Technological Privacy Tools Measure results, show that it is likely that the participants’ reported concern for cybervetting may in fact be apparent in their use of privacy settings.

When it comes to addressing these two research questions, it is hard to definitively determine whether participants have a concern for cybervetting based on the low reliability of the Likert scale items. It is apparent, however, that they have some type of concern for cybervetting and they typically employ a variety of privacy tools on their SNS, which affects their identity creation, as revealed by the Technological Privacy

Tools Measure and the open-ended responses to the Concern for Cybervetting Measure. These findings, though contradicting in some ways, speak to the messiness of social media and the nuanced ways in which individuals use it. People use social media in a variety of different ways and to achieve different goals, and as time goes on, individuals' social media use, topics they post about, and even their own circumstances, which can range from things such as the political climate, their job seeking status, relationship status, and more, is constantly changing. For example, maybe cybervetting is not as prevalent (as suggested in the Likert scale responses) for the individuals in this study because data was collected in the beginning of their senior year, as opposed to closer to graduation when job seeking is in full-swing, or maybe self-selecting or monitoring what they post on SNS is something that individuals currently do automatically and do not put much thought into, as many participants may be seasoned social media users that are already programmed to be mindful when posting on social media. In this way, this constant evolution of circumstances and social media use may do a better job of explaining these conflicting findings.

Although there is no statistically significant correlation found between the Concern for Cybervetting Measure and the CPM Social Media Scale and the Technological Privacy Tools Measure, the thematic analysis and the findings from the Technological Privacy Tools Measure still suggest that many participants in this study are certainly using their social media to manipulate their online identities for the purpose of being seen in a positive light by employers. By using different privacy tools and behaviors associated with CPM, as discovered with the CPM Social Media Scale, participants are choosing what to display or not display on SNS, which all contributes to

their identity creation. In this way, participants are ultimately engaging in facework on social media, with the goal of presenting their best selves to others, including their potential employers.

Given that participants are expressing a level of concern for cybervetting and they are using different privacy settings and tools in line with CPM to manipulate their identity to be seen positively, as facework suggests, it is interesting to explore the potential practical, ethical, and theoretical implications that can result. For example, one practical implication is that these findings point to the idea that individuals are conforming their online identities to what they believe an organization desires. As a result, individuals' social media may not be an accurate representation of their desired online identity or true selves, as it is likely that parts of their life or thoughts may be concealed or altered through CPM and facework practices, ultimately in an attempt to be viewed positively by employers.

When it comes to considering the ethical implications, there may be an ethical issue with individuals using facework and CPM strategies to not portray their true selves on social media to impress potential employers because they would essentially be deceiving others about who they really are. On the other hand, it is also important to contemplate the ethical implications of organizations' use of cybervetting in general, as it can be considered unethical behavior when they use cybervetting to illegally discriminate against potential applicants or wrongfully turn down applicants for social media related discoveries that do not have any bearing on how successful an individual would be in a position.

Aside from the ethical and practical implications, this study also stands to make theoretical contributions. First, this study fills a cybervetting research gap. Much of the previous research on cybervetting focuses why organizations use cybervetting and how it makes individuals feel, but no studies to date until now have explored how organizations' use of cybervetting actually impacts job seekers' social media use and online identity creation. This study goes beyond previous research and job seekers' negative perceptions of cybervetting to uncover how cybervetting actually impacts real social media behavior and identity. Second, this study can also be seen as extending the work of CPM and facework, as it shows that these types of identity management behaviors are being used on social media, as opposed to just in real life interactions. This study is the first of its kind to apply CPM and facework to social media cybervetting, which is ultimately an important step in understanding how cybervetting impacts job seekers' use and identity creation on social media.

Limitations & Future Directions

Although the results of this study have far reaching implications about identity creation on social media given the prevalence of cybervetting, it is also important to consider some of the limitations of this study. Most of the limitations involve the study's sample. First, the sample size was small. As a result, it was more challenging for the study to achieve statistically significant results. If the sample size had been larger, the study may have produced more significant results, especially regarding the Concern for Cybervetting Measure. Second, all the participants were only recruited from one school. Because all of the participants were from one location (Midwest) and of similar age, there may have been a lack of variance within the sample, which limits generalizability across

all populations and ages. Another limitation is due to the lack of information regarding the individuals' specific circumstances and insight into how these circumstances may have impacted social media use results. As discussed above, some of the conflicting results found between the Likert scale item correlations and the thematic analysis may be due to the nuanced and evolving ways people use social media, including individuals' circumstances. Because the study collected data from individuals during the first semester of their senior year, as opposed to closer to graduation, and the study did not account for circumstances, such as asking how current events may play a role in what individuals post about, or even asking about the specific content people post, there could be effects on how people use social media and their expressed concern for cybervetting, which have not been thoroughly explored.

Finally, a limitation of the study lies within the newly developed Concern for Cybervetting Measure that was developed for the purpose of this study. Because this scale is so new, had low reliability, and has not been rigorously tested, there may be some limitations with the measure that can only better be understood through future use and testing.

Not only should future studies replicate this study using the Concern for Cybervetting Measure to see if the measure can yield statistically significant results, but future studies should also include a larger sample size, preferably made up of different ages and different geographical locations to determine if cybervetting is something that job seekers of different ages and locations are concerned about and if it has any impact on their online identity creation and social media behavior. Future studies should also explore how specific circumstances such as the political climate, current events, and

personal status (which all impact what people may or may not post on social media) affect one's expressed concern for cybervetting and social media behavior and identity creation.

Conclusion

With the emergence of social media, there is no doubt that cybervetting has increased tremendously in popularity (Ghoshray, 2012; Perry, 2015). Although cybervetting may be a quick and efficient way to gather information about candidates and may be helpful in allowing organizations to uncover potential risks or threats that can result from hiring, cybervetting may have the potential to lead to interesting implications, including affecting the way that individuals use social media and maintain and create their online identities. Using quantitative and qualitative methods, this study explored how organizations' use of cybervetting impacts job seekers' social media behavior and identity creation. The results indicated that there are correlations between both a concern for cybervetting and social media use and a concern for cybervetting and CPM behaviors on social media. The findings also reveal that participants engage in privacy setting behaviors and alluded to manipulating the way they are presented on social media as facework and CPM suggest. However, the results do not directly reveal a significant relationship between CPM and concern for cybervetting.

While the results point to some conflicting findings, they highlight a lot of important information that is key to understanding the implications of cybervetting, and ultimately emphasize that there is more research needed to explore the effects of cybervetting further. This study shows that cybervetting has inconsistent effects on individuals, ultimately speaking to how cybervetting is still evolving as a research area,

as how it is used in organizations and how it impacts individuals' maintenance and creation of social media identities is changing.

Bibliography

- Abril, P. S., Levn, A., & Del Riego, A. (2012). Blurred boundaries: Social media privacy and the twenty-first century employee. *American Business Law Journal*, 49, 1744-1714. doi:10.1111/j.1744-1714.2011.01127.x
- Acquisti, A., & Fong, C. M. (2013). An experiment in hiring discrimination via online social networks. *Available at SSRN 2031979*.
- Anthony, W. P., Perrewe, P. L., & Kacmar, K. M. (1999). *Human resource management: A strategic approach* (3rd ed.). Fort Worth, TX: The Dryden Press.
- Barrick, M. R., Shaffer, J. A., & DeGrassi, S. W. (2009). What you see may not be what you get: Relationships among self-presentation tactics and ratings of interview and job performance. *Journal of Applied Psychology*, 94, 1394-1411. doi:10.1037/a0016532
- Basic Privacy Settings & Tools. (2015). Retrieved November 30, 2015, from <https://www.facebook.com/help/325807937506242/>
- Bedijs, K., Held, G., & Maab, C. (Eds.). (2014). *Face work and social media* (Vol. 2). LIT Verlag Münster.
- Berger, C. R., & Douglas, W. (1981). Studies in interpersonal epistemology: III. Anticipated interaction, self-monitoring, and observational context selection. *Communication Monographs*, 48, 183-196. doi:10.1080/03637758109376058
- Berkelaar, B. L. (2008) "Cybervetting (Potential) Employees: An Emerging Area of Study for Organizational Communication" Paper presented at the annual meeting of the International Communication Association, TBA, Montreal, Quebec, Canada Online.
- Berkelaar, B. L. (2010). Cyber-vetting: Exploring the implications of online information for career capital and human capital decisions.
- Berkelaar, B. L. (2014). Cybervetting, online information, and personnel selection new transparency expectations and the emergence of a digital social contract. *Management Communication Quarterly*, 0893318914541966
- boyd, d. (2006). Social network sites: my definition. Many2Many, < http://many.corante.com/archives/2006/11/12/social_network_sites_my_definition.php>(November 2006b).
- Brandenburg, C. (2007). Newest way to screen job applicants: A social networker's nightmare, *The Fed. Comm. LJ*, 60, 597.

- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2), 77-101.
- Brown, V. R., & Vaughn, E. D. (2011). The writing on the (Facebook) wall: The use of social networking sites in hiring decisions. *Journal of Business and Psychology*, 26(2), 219-225.
- Child, J. T., & Agyeman-Budu, E. A. (2010). Blogging privacy management rule development: The impact of self-monitoring skills, concern for appropriateness, and blogging frequency. *Computers in Human Behavior*, 26(5), 957-963.
- Child, J. T., Haridakis, P. M., & Petronio, S. (2012). Blogging privacy rule orientations, privacy management, and content deletion practices: The variability of online privacy management activity at different stages of social media use. *Computers in Human Behavior*, 28(5), 1859-1872.
- Child, J. T., Pearson, J. C., & Petronio, S. (2009). Blogging, communication, and privacy management: Development of the blogging privacy management measure. *Journal of the American Society for Information Science and Technology*, 60, 2079–2094. <http://dx.doi.org/10.1002/asi.21122>.
- Child, J. T., Petronio, S., Agyeman-Budu, E. A., & Westermann, D. A. (2011). Blog scrubbing: Exploring triggers that change privacy rules. *Computers in Human Behavior*, 27(5), 2017-2027.
- Child, J. T., & Starcher, S. C. (2016). Fuzzy Facebook privacy boundaries: Exploring mediated lurking, vague-booking, and Facebook privacy management. *Computers in Human Behavior*, 54, 483-490.
- Clark, L. A., & Roberts, S. J. (2010). Employer's use of social networking sites: A socially irresponsible practice. *Journal of Business Ethics*, 95(4), 507-525.
- Davison, H. K., Maraist, C., & Bing, M. N. (2011). Friend or foe? The promise and pitfalls of using social networking sites for HR decisions. *Journal of Business and Psychology*, 26(2), 153-159.
- Davison, H. K., Maraist, C. C., Hamilton, R. H., & Bing, M. N. (2012). To screen or not to screen? Using the internet for selection decisions. *Employee Responsibilities and Rights Journal*, 24(1), 1-21.
- DiMicco, J. M., & Millen, D. R. (2007). Identity management: Multiple presentations of self in Facebook. *Proceedings of the 2007 International ACM Conference on Supporting Group Work* (pp. 383-386). ACM.
- EEOC: Discrimination by type. (n.d.). Retrieved July 28, 2016, from <https://www.eeoc.gov/laws/types/>

- Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook “friends:” Social capital and college students’ use of online social network sites. *Journal of Computer-Mediated Communication*, 12(4), 1143-1168.
- Equal Employment Opportunity Commission, C. S. C., Department of Labor, and Department of Justice. 1978. Uniform guidelines on employee selection procedures. *Federal Register*, 43(166): 38290-38315.
- Floyd, K. (2009). *Interpersonal communication: The whole story*. Boston: McGraw Hill.
- Frampton, B. D., & Child, J. T. (2013). Friend or not to friend: Coworker Facebook friend requests as an application of communication privacy management theory. *Computers in Human Behavior*, 29(6), 2257-2264.
- Ghoshray, S. (2012). *Emerging reality of social media: Erosion of individual privacy Through cyber-vetting and law's inability to catch up*. *J. Marshall Rev. Intell. Prop. L.*, 12, iv.
- Global social networks by users. (2015). Retrieved November 30, 2015, from <http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>
- Grasz, J. (2012). Thirty-seven percent of companies use social networks to research potential job candidates, according to new CareerBuilder survey. CareerBuilder, April 18. Retrieved from <http://www.careerbuilder.com>
- Griffith, R. L., & Converse, P. D. (2011). The rules of evidence and the prevalence of applicant faking. In M. Ziegler, C. McCann, & R. Roberts (Eds.), *New perspectives on faking in personality assessments* (pp. 34-52). Oxford, UK: Oxford University Press.
- Haefner, R. (2009). More employers screening candidates via social networking sites. Retrieved June 1, 2011 from <http://www.careerbuilder.com/Article/CB-1337-Getting-Hired-More-Employers-Screening-Candidates-via-Social-Networking-Sites/>
- Imahori, T. T., & Cupach, W. R. (2005). Identity management theory. *Theorizing About Intercultural Communication*, 195-210.
- Jin, S. A. (2013). Peeling back the multiple layers of Twitter’s private disclosure onion: The roles of virtual identity discrepancy and personality traits in communication privacy management on Twitter. *New Media & Society*, 15(6), 813-833.
- Kluemper, D. H. (2013). Social network screening: Pitfalls, possibilities, and parallels in employment selection. *Advanced Series in Management*, 12, 1-21. doi:10.1108/S1877-6361(2013)000001200

- Levashina, J., & Campion, M. A. (2009). Expected practices in background checking: review of the human resource management literature. *Employee Responsibilities and Rights Journal*, 21(3), 231-249. DOI 10.1007/s10672-009-9111-9
- Levinson, M. (2010). Social networking ever more critical to job search success. *CIO Magazine*. Retrieved May 01, 2016, from <http://www.cio.com/article/print/598151>
- Litt, E. (2013). Understanding social network site users' privacy tool use. *Computers in Human Behavior*, 29(4), 1649-1656.
- Madera, J. M. (2012). Using social networking websites as a selection tool: The role of selection process fairness and job pursuit intentions. *International Journal of Hospitality Management*, 31(4), 1276-1282.
- Meinert, D. 2011. Seeing behind the mask. *HR Magazine*, 56: 31-32, 34, 36-37.
- Moreau, E. (2016). The top 25 social networks people are using today. Retrieved July 26, 2016, from <http://webtrends.about.com/od/socialnetworkingreviews/tp/Social-Networking-Sites.htm>
- Noe, R., Hollenbeck, J., Gerhart, B., & Wright, P. (2011). *Fundamentals of human resource management* (Vol. 4). New York, NY: McGraw-Hill.
- Pempek, T. A., Yermolayeva, Y. A., & Calvert, S. L. (2009). College students' social networking experiences on Facebook. *Journal of applied developmental psychology*, 30(3), 227-238.
- Perrin, A. (2015). Social media usage. Pew Research Center.
- Perry, J. (2015, April 15). Cyber-vetting. Retrieved August 21, 2016, from <http://insights.cyberskillscentre.com/cyber-vetting/>
- Petriches, J., Fuller, K., Marciw, K., & Conquest, S. (2015). Managing your brand. Retrieved May 01, 2016, from <http://www.appliedcommunication.org/?p=30>
- Petronio, S., & Durham, W. T. (2008). Communication privacy management theory. *Engaging Theories in Interpersonal Communication: Multiple Perspectives*, 309-322.
- Ponemon Institute. (2007). *Do human resource executives use Google and other Internet tools to obtain information about prospective job candidates?* Unpublished report.

- Reinhardt, W., Ebner, M., Beham, G., & Costa, C. (2009). How people are using Twitter during conferences. *Creativity and Innovation Competencies on the Web. Proceedings of the 5th EduMedia*, 145-156.
- Schawbel, D. (2013). Reasons why your online presence will replace your resume in 10 years. Saatavilla *www-muodossa*:< [http://www. forbes.com/sites/danschawbel/2011/02/21/5-reasons-why-your-online-presence-will-replace-your-resume-in-10-years/](http://www.forbes.com/sites/danschawbel/2011/02/21/5-reasons-why-your-online-presence-will-replace-your-resume-in-10-years/)>
- Shilling, D. (2009). *Complete guide to human resources and the law*. New York, NY: Aspen.
- SHRM (2008). Online technologies and their impact on recruitment strategies. Retrieved November 30, 2015, from www.shrm.org
- Twitter Help Center: About public and protected tweets. (2015). Retrieved November 30, 2015, from <https://support.twitter.com/articles/14016>
- Van Dijck, J. (2013). "You have one identity": Performing the self on Facebook and LinkedIn. *Media, Culture & Society*, 35(2), 199-215.
- Van Iddekinge, C. H., Lanivich, S. E., Roth, P. L., & Junco, E. (2013). Social media for selection? Validity and adverse impact potential of a Facebook-based assessment. *Journal of Management*, 0149206313515524.

Appendix A

Survey Items

Demographic Items

1. Age? (Please list): _____
2. Gender
 - Male
 - Female
 - Other
3. Ethnicity
 - White
 - Black or African American
 - Native American or Alaska Native
 - Asian
 - Native Hawaiian or Pacific Islander
 - Other
4. Major? (Please list): _____
5. Post college employment status
 - Not yet, but will in the next 6 months
 - Passively seeking
 - Actively seeking
 - Offered and accepted post-college position
 - Not seeking and unemployed
6. Do you use social media?

- Yes
- No

7. Which social media outlets do you use or have a profile on? (Check all that apply)

- Facebook
- Twitter
- Instagram
- LinkedIn
- Snapchat
- Other (please list): _____

Social Media Intensity Scale

Items and Scale

Thinking about your Facebook and Twitter Social media accounts only, please respond to the following questions:

8. Approximately how many total social media friends/followers do you have overall across your social media accounts? (Please list): _____
9. In the past week, on average, approximately how many minutes per day have you spent on social media?
- Less than .5 hours
 - .5 hour to 1 hour
 - 1 hour to 1.5 hours
 - 1.5 hours to 2 hours
 - 2 hours to 2.5 hours
 - 2.5 hours to 3 hours

- 3 hours to 3.5 hours
- 3.5 hours to 4 hours
- More than 4 hours

Thinking about your Facebook and Twitter Social media accounts only, please indicate your agreement with the following statements using the Likert scale (strongly disagree to strongly agree):

10. Using social media is part of my everyday activity.

- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree

11. I am proud to tell people I'm active on social media.

- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree

12. Social media use has become part of my daily routine.

- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree

Strongly agree

13. I feel out of touch when I haven't logged onto social media for a while.

Strongly disagree

Somewhat disagree

Neither agree nor disagree

Somewhat agree

Strongly agree

14. I feel I am part of the social media community.

Strongly disagree

Somewhat disagree

Neither agree nor disagree

Somewhat agree

Strongly agree

15. I would be disappointed if I no longer had access to social media.

Strongly disagree

Somewhat disagree

Neither agree nor disagree

Somewhat agree

Strongly agree

CPM Social Media Scale

Items and Scale

CPM Component 1: Social Media Boundary Permeability

Thinking about your Facebook and/or Twitter Social media accounts only, please indicate your level of agreement with each of the following statements using the Likert scale

(strongly disagree to strongly agree):

16. When I face challenges in my life, I feel comfortable talking about them on social media.

- Somewhat disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

17. I like my social media posts to be long and detailed.

- Somewhat disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

18. I like to discuss work concerns on social media.

- Somewhat disagree
- Disagree

- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

19. I often tell intimate, personal things on social media without hesitation.

- Somewhat disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

20. I share information with people whom I don't know in my day-to-day life.

- Somewhat disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

21. I update social media frequently.

- Somewhat disagree

- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

CPM Component 2: Social Media Boundary Ownership

Thinking about your Facebook and/or Twitter Social media accounts only, please indicate your level of agreement with each of the following statements using the Likert scale (strongly disagree to strongly agree):

*Reversed Scored

22. I have limited personal information posted on social media. *

- Somewhat disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

23. I use shorthand (e.g., pseudonyms or limited details) when discussing sensitive information so others have limited access to know my personal information. *

- Somewhat disagree
- Disagree

- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

24. If I think that information I posted looks too private, I might delete it. *

- Somewhat disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

25. I usually am slow to talk about recent events because people might talk. *

- Somewhat disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

26. I don't post about certain topics on social media because I worry who has access.

*

- Somewhat disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

27. Seeing imitate details about someone else makes me feel I should keep their information private. *

- Somewhat disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

CPM Component 3: Social Media Boundary Linkages

Thinking about your Facebook and/or Twitter Social media accounts only, please indicate your level of agreement with each of the following statements using the Likert scale (strongly disagree to strongly agree):

28. I create a profile on social media so that other users can link to me with similar interests.

- Somewhat disagree

- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

29. I try to let people know my best interests on social media so I can find friends.

- Somewhat disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

30. I allow people with a profile or picture I like to access my social media profile(s).

- Somewhat disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

31. I comment on social media to have others check out my social media profile(s).

- Somewhat disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

32. I allow access of my social media profile(s) through any of these: directories or key word searches.

- Somewhat disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

33. I regularly link to interesting websites to increase traffic on my social media profile(s).

- Somewhat disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree

- Agree
- Strongly agree

Technological Privacy Tools Usage Measure

Items and Scale

34. On Facebook and/or Twitter, have you ever:

(Check all that apply)

- Changed your privacy settings
- Deleted people from your network/friends list
- Untagged photos
- Limited certain updates to certain friends/followers
- Deleted others' comments from your profile

Concern for Cybervetting Measure

Items and Scale

Thinking about your Facebook and Twitter Social media accounts only, please indicate your agreement with the following statements using the Likert scale (strongly disagree to strongly agree) and answer the questions:

*Reversed scored

35. I am selective in who I connect with on social media.

- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree

36. (If you are selective) Please describe who you would be hesitate to connect with on social media? Why? [OPEN ENDED ITEM]

37. The audience of my social media profile(s) influences what I post.

- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree

38. (If the audience influences what you post) Describe how the audience impacts the social media content you produce. [OPEN ENDED ITEM]

39. Who would you describe as the audience of your social media profile(s)? [OPEN ENDED ITEM]

40. I rarely consider how an organization would perceive my social media profile(s).

*

- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree

41. I am concerned with how organizations that I may have a relationship with perceive my social media.

- Strongly disagree
- Somewhat disagree

- Neither agree nor disagree
- Somewhat agree
- Strongly agree

42. (If you are concerned with how organizations you may have a relationship with might perceive your social media) What are you concerned about? [OPEN

ENDED ITEM]

43. (If you are concerned) When did this concern originate? [OPEN ENDED ITEM]

Appendix B

Thematic Analysis: Hesitant to Connect

“Please describe who you would be hesitant to connect with on social media? Why?”

Code Rating Number	Code Description	Total
1	Don't know/Stranger	26
2	Employer/Potential Employer	2
3	Concern for others having access to personal information	7
4	Other	5

Participant Response	Rating Assigned
If I have never heard of the person, or don't recognize them at all then I won't connect with them because I find that strange and creepy.	1
People I don't know because they have no reason to want to follow me. I usually only connect with my friends.	1
I'm hesitant to connect with anyone on social media who I do not know in person, or who I do not have any mutual friends with, especially if they are not in my network (Marquette, high school/hometown).	1
Someone that I do not know, because I don't want them to see information about me if I don't know them. Employers because I don't want them to see certain pictures.	1, 3
I use Facebook to connect with people I know, so I am hesitant to add people I do not know at all or do not have mutual friends with.	1
Strangers and people without a profile picture	1
People whose names I know, but I do not know personally. Because I have no personal connection with them and no shared experiences, so I don't see them as somebody that I actually "know"	1

I do not like to have my social media cluttered. So if I have not spoken with someone for a while, do not expect to see them again, or do not want them as a networking source I will remove them from my social media. I am also hesitant to connect with people I do not know.	1, 4
Possible employers, used to be concerned about my family, but not anymore.	2
People I don't know.	1
People who I don't know or have no mutual contacts with. Many times these accounts are fake and they try to get personal information from connecting.	1, 3
Those who I have not personally met, those I know to update their status frequently, and those people that I am not interested in updates from.	1, 4
I don't know them	1
If I don't recognize someone's name or profile picture I am reluctant to add them on social media.	1
I do not accept requests from people I do not know because I do not have an interest in seeing what they post and I am not sure how they found my profile.	1
People I don't know because if I don't know them on person I wouldn't want don't want just an internet relationship	1
I don't know why they know and if something I say or do could adversely affect me.	1, 3
Individuals much older than myself. Social media is shorthand conversation, and they usually tend to ramble on for days.	4
People I have not met and have no mutual friends with. Typically, I will not accept a friend request from a person I do not recognize at all.	1
People I don't know of and who are complete strangers.	1
Contacts just met.	4
People I do not know because they are strangers and I don't want them to have access to my information.	1, 3
Anyone who I do not know or does not have any mutual friends with me because I question their motives for wanting to friend me	1, 3
Anyone I don't know, because people are crazy and can hide behind fake profiles. I'm not stupid. I only have acquaintances on my social media.	1

Someone I don't know.	1
Employer. Want to keep social and professional lives separate	2
People I do not know personally	1
Strangers because I don't know them and they have no reason to know about my personal and social life.	1, 3
People who are overly political one side or another.	4
I would be hesitant to connect with someone if it were somebody that I did not have any interaction with on a daily basis or know something about them	1
Someone I don't know and have limited mutual friends with because I don't want them to have access to anything in my profile that isn't available to people who are not my friends	1, 3

Appendix C

Thematic Analysis: Audience Impact

“Describe how the audience impacts the social media content you produce.”

Code Rating Number	Code Description	Total
1	Employer/Potential Employer/Co-workers	6
2	Like-minded individuals/What people want to hear	5
3	Not-offensive/Content that others do not approve of	5
4	Set an example	2
5	Parents/Family	4
6	Other	6

Participant Response	Rating Assigned
Since I know that potential employers as well as my parents and their friends are looking at my social media pages, I would not post anything with offensive language, and I definitely don't share the kind of personal details I would share with a close friend.	1, 3, 4
My audience is people I associate with meaning they are like-minded. They influence sharable content. Some of my ideas stem from their own.	2
I tailor my posts to what I think people might like to hear or need to hear (like words of encouragement or positive thoughts or funny stories)	2
I don't want to post inappropriate items, or things my audience would not approve of	3
I am friends with coworkers and friends and do not post things I wouldn't want to share with them in conversation.	1
I need to stay relevant and leverage social media to grab people's attention	6

<p>It depends on the platform. Twitter I'm very political and don't care what I say even though its more open and more strangers could see what I wrote(though I keep my name off the profile), whereas Facebook is very personal and I tend to talk about positive things instead.</p>	6
<p>I do not like to post things that I know will be outright offensive to different audiences. I am also conscious of the professional nature that must go along with social media.</p>	3, 1
<p>I used to be a camp counselor and I allowed my campers to "friend" me. I know I set an example for them so I don't want to set a bad example. Additionally, I don't want my co-workers to see me out partying or kissing my boyfriend on the internet</p>	1, 4
<p>I'll be more careful about what I say.</p>	6
<p>Although I do not like to think about having a particular image, I think it is important to maintain a respectful image and reputation especially since family members and younger children who look up to me have connected with me on social media.</p>	4, 5
<p>I know that my main audience on my social media accounts is my friends, so I try to keep my captions funny and posts entertaining. I rarely go into big political or social rants because I would rather have those conversations in person.</p>	2
<p>On Facebook I have both friends, family, and past co-workers so I try to keep my content as PG as possible. My posts are also a lot less frequent. I do have to watch what kinds of things I'm tagged in, etc. On Twitter, it's almost all friends of mine from college and high-school and a variety of news sources or parody accounts. My twitter is almost impossible to find to someone who does not know me personally, so there is definitely less filter</p>	1, 5
<p>It really does not impact what I produce, just what I am willing to share. Information that I find which raises awareness of issues I find important, or something which pertains to my relationship with my audience may be shared. Private information such as travel plans, photos of family, or personal issues are not.</p>	6
<p>I am selective about what I post depending on who has access.</p>	6
<p>I won't post something if I know it's controversial</p>	2, 3
<p>I don't post the same thing depending on the audience</p>	6
<p>Appropriateness</p>	3

I post things I am comfortable with my family seeing	5
I have to remember I'm friends with my parents on Facebook. Anything I wouldn't want them to see I don't post.	5
I don't want the adults/future employers seeing inappropriate pictures	1
I care about their opinions on my posts.	2

Appendix D

Thematic Analysis: Audience of Social Media

“Who would you describe as the audience of your social media profile(s)?”

Code Rating Number	Code Description	Total
1	Friends	38
2	Family	26
3	Co-workers	6
4	Other	8

Participant Response	Rating Assigned
A lot of school friends, some moms and grandparents and friends of my parents.	1, 2, 4
My friends or friends of friends.	1
My friends, classmates, family members, family friends, and acquaintances.	1, 2
My personal friends, acquaintances, classmates and old friends.	1
My family, friends, peers/classmates from high school and college.	1, 2
Friends/Family	1, 2
My friends and acquaintances	1
Friends and people I've met. These people know who I am and understand the type of person I am, so I feel comfortable posting whatever because it keeps shaping the perception of me that people have and helps them know me even better.	1
Either friends that I have met or that I am very close with or bots.	1, 4
Friends	1
Friends, family, and fellow coworkers	1, 2, 3

Friends, family, acquaintances	1, 2
My family, close friends, long-time friends, new friends. No strangers.	1, 2
Family, friends, coworkers.	1, 2, 3
Students and millennials	1, 4
Friends	1
Family and friends	1, 2
Friends and family=Facebook / Political likeminded people=Twitter	1, 2, 4
Friends and family	1, 2
Family and friends	1, 2
My friends! only. I make friends at work, so some are both friends and co workers	1, 3
Friends, co-workers, family	1, 3, 2
People who are interested in Sports.	4
My audience would mainly be my peers and my family. Although the majority of my audience is my friends/peers, those who tend to interact with me the most on social media are my family.	2, 1
My friends mostly and some family.	1, 2
Friends, family, possibly prospective employers (FB, LinkedIn)	1, 2, 3
Those people who I know or have known in person.	1
Friends who share my interests, though not necessarily my own views. Includes multiple Jesuits, overseas friends from the middle east and high school contacts who I perceived as people who I might help, or might help myself further down the road.	1, 4
Friends and family	1, 2
Friends and family	1, 2
Facebook - No one. I rarely use it. / Snapchat - close family and friends.	1, 2
Facebook, friends and family / Twitter, Wild card / Instagram, creative people / Snapchat, mix of the above / Linked In, barely anyone	1, 2, 4
Friends and family	1, 2
Friends and family	1, 2

Family and friends from school and work now and past	1, 2, 3
Friends, family, mentors	1, 2, 4
Friends, family	1, 2
Friends, family	1, 2
Anyone who is a friend of mine online	1

Appendix E

Thematic Analysis: Concern about Posting

“What are you concerned about?”

Code Rating Number	Code Description	Total
1	Job/Employer Related/Professionalism	14
2	Appropriateness of posts/Offensive/Perception	10
3	No concern	2
4	Disapproval/Don't agree	3
5	Other	1

Participant Response	Rating Assigned
I am nervous about not getting a job due to social media so I try to be thoughtful through my posts.	1
If my pictures are inappropriate to potential employers.	1
Employers viewing my pictures from weekends of going out drinking.	1
I am concerned about how appropriate my posts may be to outsiders and professional connections	1, 2
I am concerned about posting inappropriate content (pictures, words, post) and also controversial topics. I will post what I strongly feel is right. This could be controversial topics, but I am not fully concerned because some topics become a part of me which is difficult to change. If a job cannot take me as I am, then I am not the right fit for that organization. For example, I support the Black Lives Matter movement and actively post in regards to the ethical treatment of beings of color without hesitation.	2
Nothing	3
Looking unprofessional or just being obnoxious on social media	1
Posting items that might offend others or cause others to be cruel to me.	2

Them seeing content they disapprove of	4
There is no current concern, but I tend to keep personal opinion posts off Facebook because not all of my Facebook friends share the same beliefs, ethics and morals as I do. I'd rather not offend or upset people.	2
I am concerned of the perception I might give off based on what pictures I post or status' I put out there.	2
Negative or inappropriate content	2
Unprofessional content	1
Employers or friends who don't agree with me, judge me differently online than how I am to them in real life.	4
Working in a hospital means that I am privy to a lot of sensitive, confidential information, so I will not post anything about that. I am also concerned for my future employment and my social media must reflect the professional person that I am.	1
I want to stay respectful online and offline. I want my employers to search me and not be turned off by what they see (even if they can't see anything due to privacy settings) and I am friends with my family members so I wouldn't want to post anything I wouldn't feel comfortable talking to them about	1
I am concerned about people drawing false assumptions from my profiles.	2
N/A	3
I am concerned of friends on social media who may "tag" me or "comment" something inappropriate on my page.	2
Privacy is a very large concern when it comes to social media. Information may be distributed at the drop of a hat and so my greatest concern is my own self-restraint when it comes to interacting with such a wide and diverse audience. / / Knowledge is power, but wisdom is priceless.	5
I want to make sure I keep a professional appearance.	1
Losing a job for showing illegal actions (ex. underaged drinking), and getting retaliation for something they don't like.	1
Opinions	4
Professionalism	1

Them (organizations) seeing photos they don't need to see of me, even if they are harmless I just want to keep my social life separate.	1, 2
They (organizations) will see inappropriate immature pictures of me going out	2
How the organizations view me.	1
Maintaining a somewhat professional profile on Facebook so that future employers may not be driven away from what could be a harmful post	1

Appendix F

Thematic Analysis: Concern Origination

“When did this concern originate?”

Code Rating Number	Code Description	Total
1	Job/Potential employer related	10
2	In college/high school	10
3	None	2
4	Other	4
5	Always	4

Participant Response	Rating Assigned
My dad instilled this concern in me because he is on the hiring board for his company.	1
When I came to college and was concerned with finding a job.	1, 2
When I got to college.	2
When I started looking for jobs in high school, some people told me that job recruiters may look at potential employees' social media.	1
In college	2
N/a	3
By seeing too many people have annoyingly long and unimportant posts about stuff I don't care about their opinion of.	4
This has always been my concern from the start of having social media accounts.	5
Teachers, parents said to be careful, mid high school	2
Before I created a Facebook profile.	5

As I have gotten older, and especially once I went to college, I was very careful with what pictures I posted and was tagged in.	2
My first PR class	2
My profile has always been sparse. Now that I am job-seeking I am even more aware.	1
My parents were big on keeping private matters private. So naturally I guess I inherited some of this.	5
When I became friends with older family members I started censoring my content more.	4
I think I once read an news article about someone getting fired because they trashed their company on social media	1
From hearing discussions about organizations using social media profiles to gather information on people, especially potential employees.	1
N/A	3
Just simply by the diversity of friends and mentalities that friends on social media have.	4
This concern originated when I first joined social media, discovering just how much people were willing to share about themselves and realizing how vulnerable a position they put themselves in unconsciously.	5
My second year at college	2
2009 - I was far ahead of my counterparts when considering my future successes.	4
When I started looking for jobs	1
Job seeking	1
College	2
High school	2
Entering college and considering applying for jobs.	1, 2
Upon learning that employers can check Facebook profiles while looking for job candidates	1