

FAIRNESS PERCEPTIONS OF SCREENING SOCIAL NETWORKING SITES FOR
HIRING DECISIONS

by

Kimberly E. Kluesner

A Thesis submitted in Partial Fulfillment
of the Requirements for the Degree of
Masters of Arts in Industrial and Organizational Psychology

Middle Tennessee State University

August, 2013

Thesis Committee:

Dr. Patrick McCarthy

Dr. Judith Van Hein

Dr. Michael Hein

ACKNOWLEDGEMENTS

I would like to first thank my family and friends for all of the support you have given me. I would not be where I am today without all of you. I especially want to thank Chris for moving to Tennessee and being there for me through it all. You believed in me when I did not always believe in myself and I could not have done it without your love, support and patience during these past two years. I would also like to acknowledge my thesis committee for your guidance and diligence during the process of completing this thesis. Your advice and direction truly made the difference. Especially Dr. Patrick McCarthy who was instrumental in this thesis process and who I saw as a mentor throughout my graduate school experience. Your eternal optimism and belief in my abilities kept me progressing and persevering to the very end and for that I thank you.

ABSTRACT

As the popularity of social networking sites (e.g. Facebook and Twitter) continues to increase, employers are beginning to use these sites as sources of screening applicants for hiring purposes. Employers feel the need to screen the sites due to a number of legitimate business concerns related to hiring applicants including illegal activity such as drug use and inappropriate behavior such as negative work comments about one's current workplace. However, there are concerns with the level of privacy invasiveness employers are using to find this information such as requiring login information. This study's primary focus was to determine if levels of privacy invasiveness and legitimate business concerns would influence fairness perceptions. Higher levels of privacy invasiveness and less serious levels of the legitimate business concerns found resulted in lower fairness perceptions. Results indicate potential issues employers may encounter as they attempt to balance their legitimate business concerns with applicants' privacy concerns.

TABLE OF CONTENTS

LIST OF TABLES	vi
LIST OF FIGURES	vii
CHAPTER I.....	1
Introduction.....	1
Social Networking Sites.....	2
Screening Social Networking Sites.....	3
Advantages to Screening Social Networking Sites.....	4
Risks of Screening Social Networking Sites	8
Potential Solutions	23
Current Study	28
Primary Research Focus	29
Additional Hypotheses.....	30
CHAPTER II.....	31
Method	31
Participants.....	31
Design	33
Procedure	35
Measures	36
Materials	37
CHAPTER III	42
Primary Results.....	42
Correlational Analyses.....	42
Preliminary Analyses	42
Primary Analyses	43
Primary Hypothesis Testing.....	51
Additional Results.....	52
Control Condition Analyses.....	52
Social Networking Site Usage Analyses.....	53
Applicant Screening Experience Analyses	53

Additional Hypothesis Testing	54
CHAPTER IV	56
Discussion	56
References	62
APPENDICES	67
Appendix A: Survey Instrument	68
Appendix B: Ethnicity	77
Appendix C: Job Level	78
Appendix D: Social Networking Site Accounts	79
Appendix E: Average Time Spent on Social Networking Sites	80
Appendix F: Average Time Spent on Social Networking Sites Daily.....	81
Appendix G: Applicant Experiences	82
Appendix H: Correlations	83
Appendix I: Scale Reliability.....	84
Appendix J: IRB Approval	85

LIST OF TABLES

Table 1. 3x3 Factorial Design for Privacy Invasiveness and Drug Use	34
Table 2. 3x3 Factorial Design for Privacy Invasiveness and Negative Work Comments	35

LIST OF FIGURES

Figure 1. Process Fairness of Drug Use and Privacy Invasiveness	44
Figure 2. Decision Fairness of Drug Use and Privacy Invasiveness	46
Figure 3. Process Fairness of Negative Work Comments and Privacy Invasiveness	48
Figure 4. Decision Fairness of Negative Work Comments and Privacy Invasiveness	50

CHAPTER I

Introduction

With the emergence and increasing popularity of social networking sites such as Facebook, Twitter, and LinkedIn, more human resource personnel and employers are utilizing the information that is available on those sites (Brown & Vaughn, 2009). Employers are increasingly using social networking sites as a tool for screening job applicants (Brown & Vaughn, 2011; Elzweig & Peeples, 2009; Slovensky & Ross, 2012; Waring & Buchanan, 2010). However, with new technology comes the responsibility for addressing related controversies about significant risks and benefits at both the practical and ethical levels.

Although employers have a responsibility to be diligent in hiring practices in order to avoid negligent hiring, there is also a possibility of misusing the information that is provided by social networking sites (Elzweig & Peeples, 2009; Waring & Buchan, 2010). Whether this misuse of the information is intentional or not, employers are taking risks and making themselves vulnerable to potential legal ramifications. By using information from sites such as Facebook to screen applicants, employers are potentially violating privacy rights, obtaining misleading or incorrect information about an applicant, and receiving protected information that a human resource professional otherwise would not inquire about due to the relevant employment laws (Brown & Vaughn, 2011; Elzweig & Peeples, 2009; Slovensky & Ross, 2012; Waring & Buchanan, 2010).

These issues and controversies are beginning to emerge in the research and among legal cases and will only continue to grow in number. Because of the recent emergence

of these controversies, it is important to discuss the significant employment and privacy protections that may apply to social networking. It would also be useful to determine what the current perceptions and expectations are in the workplace on what is considered fair or unfair when using social networking information during the hiring process and if there are individual differences among those perceptions (Clark & Roberts, 2010; Waring & Buchanan, 2010). This research can provide employers with information about what applicants feel is fair and what practices may be more acceptable and/or aid in reducing the possible legal issues for their companies.

Social Networking Sites

“Social networking sites allow users to create web-based profiles where individuals can interact” (p. 220) with one another and choose with who they share information (Brown & Vaughn, 2011). Social networking sites (SNS) can include but are not necessarily limited to blogs, photo-sharing sites such as Tumblr, Internet forums, and social profiles such as Facebook and Twitter (Lanham, 2010). Users of SNSs create a personal profile that may contain a variety of content including images, biographical information, posts by the user, and more (Brown & Vaughn, 2011). Each user has a “network” in which they have given access to certain people to view their profile information, sometimes called “friending.” How much information people in their network or out of their network are able to see on their profile, may depend on the privacy settings set by the user (Brown & Vaughn, 2011). Although most social networking sites are used for recreational purposes, more and more employers are seeing the value in screening these sites for employment reasons.

Screening Social Networking Sites

Previously, the norm for employers was to conduct background checks only for serious candidates as a business necessity. However, with the growth of the Internet and social networking sites the shift has been to conduct a background check informally through SNSs for most applicants (Clark & Roberts, 2010). Due to the rise of social networking sites, such as Facebook and Twitter, employers have access to more personal information about applicants than ever before (Sronce, 2011). Information found on social networking sites is being used in conjunction with traditional application materials such as résumés and cover letters in order to make hiring decisions (Bohnert & Ross, 2010).

Online screenings of applicants' SNS profiles allow the employer to get a quick character check of the applicant and gather additional information for hiring purposes beyond traditional application materials (Clark & Roberts, 2010; Davison, Maraist, & Bing, 2011; Sronce, 2011). This information may be used to screen out individuals, screen in individuals, or develop targeted questions for an interview (Davison, Maraist, & Bing, 2011). Applicants have been screened out of jobs due to information provided on SNS profiles. SNS information that has been found to screen out an applicant are: inappropriate or risqué pictures, poor communication skills indicators, alcohol or drug use indicators, information that falsifies résumés, and posts criticizing co-workers or current employers (Brown & Vaughn, 2011). Applicants also have the potential to increase their chances at a job position with information provided on SNS profiles. SNS information that has been used to screen in an applicant are: information supporting qualifications for the job, displaying characteristics that make them a good fit with the

organization, showing strong communication skills, and displaying creativity (Brown & Vaughn, 2011).

Advantages to Screening Social Networking Sites

Negligent Hiring

Employers feel they have a responsibility to conduct online checks in order to protect themselves from negligent hiring (Clark & Roberts, 2010; Elzweig & Peeples, 2009; Slovinsky & Ross, 2012). Employers must do everything legally possible to screen out applicants that may cause avoidable harm in the workplace, known as due diligence (Johnson, 2011; Waring & Buchanan, 2010). Negligent hiring occurs when an employer does not conduct due diligence in an attempt to fully uncover an applicant's incompetence, criminal background, or other relevant information that may influence the company negatively by that employee later causing harm to others while the person is working for the company (Clark & Roberts, 2010; Slovinsky & Ross, 2012). Criminal background checks are often done for this reason. However, a person may still engage in questionable behaviors even if they do not have a criminal record, and a SNS profile may provide evidence of those behaviors to employers (Slovinsky & Ross, 2012).

The recent court decisions have stated that Google searches and other Internet searches should be part of due diligence by the employer (Elzweig & Peeples, 2009). However, it is important to note that part of preventing negligent hiring is to take reasonable action, and it is yet unclear how far an employer can or should look into SNS profiles to meet and not overstep this criterion (Waring & Buchanan, 2010). Employers may access sites in a variety of ways, including having employees with the same social network as the applicant to try and bypass network settings and possibly "friend" them

under these pretenses. Some employers may even create “pseudo-profiles” to attempt to gain access to an applicant’s SNS profile (Elzweig & Peeples, 2009). It is still unclear what specific SNS screening practices may or may not be legally defensible.

Information Verification

In addition to preventing negligent hiring, there are other advantages to screening an applicant’s SNS profile (Bottomly, 2011; Brown & Vaughn, 2011; Kluemper, Rosen, & Mossholder, 2012; Slovensky & Ross, 2012). Information on SNSs may provide more honest information than traditional cover letters and résumés, which are meant to highlight a person’s best characteristics (Slovensky & Ross, 2012). Many résumés actually include incorrect or exaggerated information (Slovensky & Ross, 2012). SNS profiles may provide an opportunity for an employer to verify information from a résumé (Brown & Vaughn, 2011; Slovensky & Ross, 2012). It has also been suggested that screening SNSs may be more cost-effective in the early stages of the selection process than the cost of an extensive background check (Slovensky & Ross, 2012). Minimal to no cost is required to find information about a candidate through SNSs (Bottomly, 2011; Brown & Vaughn, 2011).

Correlates to Personal Characteristics

Screening an applicant’s SNS profile may also provide a “big picture” of the applicant in order to determine fit with a company or job (Bottomly, 2011). It has been suggested that an applicant’s profile on a SNS can provide information to help determine fit with the organization or position. Characteristics that may possibly be determined using SNS profiles are personality, intelligence and potential global performance that the employer would not be able to infer from traditional application materials (Brown &

Vaughn, 2011; Davison, Maraist, & Bing, 2011; Kluemper & Rosen, 2009). These inferences are then used to determine correlates to potential job performance which may influence hiring decisions (Davison, Maraist, & Bing, 2011). However the ability to infer personality and other characteristics from a SNS has not been extensively studied to date (Kluemper & Rosen, 2009).

In a study by Kluemper and Rosen (2009), initial evidence supporting the validity of using SNS information to determine personality, intelligence, and global performance was found. In their study, raters of individuals' SNS profiles were able to make inferences similar to the individuals' self-reported personality, intelligence, and global performance. Interrater agreement was also found supporting the reliability of SNS information (Kluemper & Rosen, 2009). Conscientiousness in particular has been found in the literature to be a good predictor of overall job performance (Kluemper & Rosen, 2009). Cognitive ability has also been found to be a predictor of individual performance at work (Kluemper & Rosen, 2009). A SNS profile may allow an employer to determine if the applicant has these characteristics that correlate to job performance. This research provided some support for using SNS information to determine personality and other characteristics of potential applicants. In a later study, Kluemper, Rosen, and Mossholder (2012) found similar results that SNS information may be appropriate for determining applicant personality. It was found that self-ratings, as well as others' ratings, are fairly accurate in measuring personality from SNS information (Kluemper, Rosen, & Mossholder, 2012).

Influence on Hiring Decisions

There have been few studies empirically studying how social networking site information influences employment decisions (Bohnert & Ross, 2010). In their study, Bohnert and Ross (2010) found that having an alcohol-oriented SNS resulted in the lowest desirability for hire rating as compared to a family-oriented profile, professional-oriented profile, and having no SNS profile. Results also showed that if an applicant with an alcohol-oriented SNS was offered the job, raters would offer a lower salary to them than they would to an applicant with a more appropriate SNS orientation (Bohnert & Ross, 2010). It was also found that SNS information can enhance a candidate's desirability compared to someone who does not have a SNS. If the applicant's SNS was professional- or family-oriented, they were rated as more desirable to hire than someone without a SNS profile. The results of Bohnert & Ross' (2010) study suggested that SNS information does influence how an applicant is evaluated and can influence hiring decisions, such as wages offered, and whether the applicant receives a job offer or not (Bohnert & Ross, 2010).

SNS information may also reinforce initial impressions or decisions based on other information such as a cover letter or résumé (Elzweig & Peeples, 2009; Slovensky & Ross, 2012). Elzweig and Peeples (2009) stated that employers may use SNS information to confirm an initial impression they received when reviewing other application materials and may ignore information that does not adhere to that initial impression, called a confirmation bias. It has been suggested that if SNS information is the first information that an employer receives about an applicant, it may have a heavily

weighted influence over their decision, even if other information is provided later on that is contrary to that initial impression (Slovensky & Ross, 2012).

Unfortunately, it has yet to be determined if decisions based on SNS information are actually translated to the workplace (Clark & Roberts, 2010; Davison, Maraist, & Bing, 2011). There is a lack of theoretical constructs which makes it difficult to determine what information is actually influencing the hiring decision (Brown & Vaughn, 2011). There has not been any research validating the information that is gained from SNSs by employers for hiring purposes. This lack of validation may increase potential legal repercussions (Brown & Vaughn, 2011).

Risks of Screening Social Networking Sites

Many agree that there are a variety of legal and practical risks that are taken when an employer screens a SNS profile for hiring decisions (Bottomly, 2011; Brown & Vaughn, 2011; Clark & Roberts, 2010; Davison, Maraist, & Bing, 2011; Dennis, 2011; Elzweig & Peeples, 2009; Johnson, 2011; Kluemper & Rosen, 2009; Slovensky & Ross, 2012; Sronce, 2011). The major concerns with screening SNS information are inaccurate or incomplete information, misidentification, fairness perceptions, privacy issues, and discrimination claims. Currently there are few court decisions referring to employer liability when they utilize a SNS for screening, and there are no federal laws that directly address these issues with SNSs. Moreover, published empirical research is very limited regarding the legal and practical ramifications for employers using this information for hiring purposes (Brown & Vaughn, 2011; Elzweig & Peeples, 2009; Johnson, 2011).

Inaccurate or Incomplete Information

A risk that employers take when screening SNS information is receiving inaccurate or incomplete information about a candidate (Dennis, 2011; Elzweig & Peeples, 2009, Slovensky & Ross). The information provided on a site may not be accurate because of a variety of reasons. The profile may be falsified or created to make the applicant appear better or worse than they are depending on the intended audience (Johnson, 2011). In other words, individuals may try to “fake good” or “fake bad” on their SNS profile, depending on whom they expect to view the profile (Davison, Maraist, & Bing, 2011).

Previous research has shown that the social norm of most SNSs is to emphasize exaggeration and outlandish behavior, and postings by applicants may reflect that norm (Slovensky & Ross, 2012). Information on SNS profiles may also be outdated and may represent what an applicant was like in a different phase of their life and may or may not represent what they are like today (Slovensky & Ross, 2012). Due to these reasons, an applicant’s profile may not accurately reflect what they may be like as an employee today (Slovensky & Ross, 2012). Using information for hiring purposes from SNSs can lead to unfair inferences due to the possibility that the information may be inaccurate (Waring & Buchanan, 2010). The legality of using this information has been called into question and requires more study (Davison, Maraist, & Bing, 2011).

Misidentification of Applicants

There is also no way of determining if the applicant was actually the one who posted the information on the SNS profile (Dennis, 2011). An employer cannot even be sure if the profile they are viewing is the applicant or someone with the same name

(Johnson, 2011). Because of the popularity of SNSs, it is possible that the profile an employer is looking at is not actually the applicant's but is a profile of someone who has a similar name (Slovensky & Ross, 2012; Sronce, 2011). Mistaken identity is common among SNSs and is also ripe for imitation accounts or attempts to sabotage another applicant's chances at a prestigious or highly competitive job position (Slovensky & Ross, 2012). There are people called "profile poachers" who create fake profiles of individuals and may use that opportunity to act maliciously against them (Sronce, 2011). An applicant who knows their competitors for a job position may try to sabotage their chances of receiving the job offer by poaching their SNS profiles (Sronce, 2011).

Fairness Perceptions

Another concern for using SNS information is the fact that it can influence fairness perceptions in both the outcome and the procedures of selection (Slovensky & Ross, 2012). Distributive justice refers to whether or not an applicant may believe the outcome was fair (Slovensky & Ross, 2012). Procedural justice refers to whether or not an applicant may believe the procedures taken to make the decision were fair (Slovensky & Ross, 2012). Part of procedural justice is how information is utilized in decision making and what information is provided to the applicant on why a certain decision was made (Slovensky & Ross, 2012).

An applicant who discovers their SNS information was screened may feel that their privacy had been violated, and thus perceive that practice as having low procedural justice (Slovensky & Ross, 2012). In a study by Bauer et al. (2006) it was found that procedural justice mediated the relationship between privacy concerns and applicant reactions including test-taking motivation, organizational attraction, and organizational

intentions. These perceptions of justice can influence an applicant's decision to accept or reject a job offer (Bauer et al., 2006; Slovensky & Ross, 2012). They may choose to reject an offer if they feel the procedure was unfair or had at some point violated their privacy (Bauer et al., 2006; Slovensky & Ross, 2012). Applicants may feel that employer's use of screening SNSs for hiring decisions is unfair due to the recreational nature and social purpose of a SNS (Sronce, 2011). It may also negatively influence their customers' perceptions of the company if they find out about the practice and feel the practice is unfair (Bauer et al., 2006). These nuances of justice perceptions have not been thoroughly studied in relation to SNS screening, but they are expected to have an impact on employers who screen SNSs (Slovensky & Ross, 2012).

Invasion of Privacy

The issue of potentially violating privacy rights is one of the main controversies in relation to utilizing SNS information for hiring decisions (Brown & Vaughn, 2011; Clark & Roberts, 2010; Davison, Maraist, & Bing, 2011; Dennis, 2011; Slovensky & Ross, 2012; Sronce, 2011). Employers are taking a variety of measures to gain access to information from SNS profiles that may or may not be violating the individual's right to privacy. For example, employers may ask a current employee to "friend" an applicant on a SNS in order to gain access. However, this may result in an invasion of both the applicant's and the employee's privacy rights. It may also lead employees to engage in fraudulent behavior (Slovensky & Ross, 2012). Employers who attempt to circumvent privacy protections may be liable for these privacy violations (Dennis, 2011).

It has been suggested that viewing profiles with user-controlled privacy settings may be an invasion of that individual's privacy and "likely violates the terms and

conditions of most social networking sites” (Bottomly, 2011, p. 2). It has been argued that when a SNS user places information on a public domain they waive their reasonable expectation of privacy (Clark & Roberts, 2010). Because of this viewpoint, most claims of invasion of privacy in these situations would fail due to the voluntary disclosure of information to the public (Dennis, 2011). However, for privacy in SNSs, Clark and Roberts (2010) point out that it is important to distinguish between self-presentation and self-disclosure. Self-presentation is information about the individual that they allow to be public. Self-disclosure is information the individual takes an active role in preserving so that not everyone may have access to it. It is suggested that employers should only access self-presentation information.

Definitional Issues

Unfortunately, there is a lack of definition for what constitutes privacy and what does not in regards to SNS profiles (Clark & Roberts, 2010). However, in the case of *Katz v. United States* (1967) the courts stated that two requirements must be met for an invasion of privacy to be a legitimate claim. First, the individual must display an expectation of privacy. Second, the expectation of privacy should be recognized by society as being reasonable (Clark & Roberts; 2010; Elzweig & Peeples, 2009). If the information is publicly available then it is well agreed upon that they do not have a reasonable expectation for privacy. However, the controversial debate occurs when the individual has utilized SNS privacy settings in order to restrict the access of others to their information (Clark & Roberts, 2010; Lanham, 2010).

Privacy Settings

A person's expectation of privacy when using social networking sites depends on how they set up their account and the conditions of privacy the site has (Elzweig & Peeples, 2009). A SNS user who took the necessary steps to restrict access to their profile may have a higher expectation of privacy than those who do not. In the case of *Pietrylo v. Hillstone Restaurant Group* of 2009, a federal district court in New Jersey ruled that an employer's unauthorized access to restricted SNS postings violated the Stored Communications Act because "an employee may have a reasonable expectation of the privacy of the communications or information" (p.2) if they actively pursue restricting access to others through SNS privacy settings (Lanham, 2010). This may correspond to reasonable expectation of privacy for an applicant as well, if they take the necessary steps to restrict access to their SNS profiles. In future court decisions regarding SNS information, the courts will attempt to balance these reasonable expectations of privacy versus the relevance of the information that an employer is entitled to for hiring decisions (Dennis, 2011).

However, SNS policies such as those used by Facebook state that individuals should use the site at their own risk, and that not all privacy measures are perfect. Because a user agrees to the policy when they create a SNS profile, these statements may influence whether or not a person can have a privacy violation claim or not (Elzweig & Peeples, 2009). However, Facebook has recently taken action to help protect its users against employers who seek access to the applicant's password in order to access restricted areas. In a recent posting on their website, Facebook stated "This practice undermines the privacy expectations and the security of both the user and the user's

friends. It also potentially exposes the employer who seeks this access to unanticipated legal liability” (Egan, 2012). Facebook has since made it a violation of their Statement of Rights and Responsibilities to share or solicit a Facebook password. Facebook has gone as far as threatening legal action against those employers who attempt to solicit applicants’ passwords (Egan, 2012).

Although the federal government has not directly addressed this issue, there is a rising trend of states that are proposing legislation which would help protect applicants’ passwords. Maryland was the first state to pass a law banning the solicitation of applicants’ passwords. Maryland’s House Bill 964 was proposed after the American Civil Liberties Union (ACLU) formally complained about the Maryland Department of Public Safety and Correctional Services requiring Facebook login information of a current employee. The bill made it unlawful for employers to ask for any login information in order to access a personal account or service through an electronic communications device (Martucci & Shankland, 2012).

Legislation has also been introduced recently at both the federal and state levels. As of 2013, at least eight more states have joined Maryland in passing such legislation, including Arkansas, Illinois, California, Michigan, New Jersey, Utah, New Mexico, and Delaware (Greenberg, 2013). For example, Illinois Governor Pat Quinn signed House Bill 3782 into law (Ahearn, 2012a). The law bans employers from applying any manner of seeking account access, not just login information (Martucci & Shankland, 2012). In another example, Assembly Bill 1844 was passed in California’s state Assembly and signed into law on September 27th, 2012 by California Governor Edmund G. Brown Jr. (Martucci & Shankland, 2012; Ahearn, 2012b). This law bans employers from requiring

disclosure of login information by an applicant or employee. Employers can still request this information but this law protects applicants who decline to provide the information (Martucci & Shankland, 2012).

Congress has also begun to notice the issue of employers asking for login information. In May of 2012, the Password Protection Act of 2012 was introduced in both the U.S. Senate and House of Representatives. Similar to California's bill, the Act would not ban employers from requesting login information but would prohibit requiring the information be disclosed or provided access to. It would also prohibit "discharging, disciplining, or discriminating against employees for refusing to grant access of such information" (Martucci & Shankland, 2012, p. 82). While Congress did not come to agreement on this bill in 2012, they have continued their efforts to develop it in 2013 (Library of Congress, 2012).

Privacy Legal Protections

Currently, the most common privacy protection cited is the Stored Communications Act (SCA) of Title II of the Electronic Communications Privacy Act (ECPA). In the situation where an individual has a legitimate privacy claim in regards to electronic communication access without authorization, the SCA may apply to SNS screening (Dennis, 2011; Lanham, 2010). The ECPA provides protection but is often interpreted by courts narrowly (Clark & Roberts, 2010). The Stored Communications Act states that it is illegal to "intentionally access without authorization a facility through which an electronic communication service is provided." 18 U.S.C. §§ 2701-2711 (2000) (Elzweig & Peeples, 2009, p. 30). The SCA restricts unauthorized access to information on an electronic communication service that is maintained by a third-party provider.

This can include password-protected social networking groups or information hidden from public view via privacy settings (Lanham, 2010). The SCA could potentially influence liability of employers screening SNSs (Morin & Arce, 2011). Recent court cases have determined that private SNS messages are protected under the SCA. These messages also cannot be subpoenaed for use in civil litigation (Dennis, 2011). The SCA prohibits electronic communication service providers from disseminating private messages on a SNS that are not publicly accessible (Morin & Arce, 2011). Employers accessing this information may be in violation of the SCA.

The SCA does include an exception whereby the user authorizes a service with communication they provided. In a situation where an employer asked a current employee to “friend” an applicant on a SNS and the friend request is accepted by the applicant, then that employee has gained authorized access. In this case the exception would likely apply if there was no pressure put on the applicant to accept the friend request and it was strictly voluntary. This would then allow the employer to view an applicant’s profile without violating the SCA. However, even unintended coerciveness would result in a violation as long as the applicant felt pressure to accept, leading the court to view it as coerced access. However, other protections outside of the SCA may still hold true for this situation. Even if there are not legal protections in place, the deception of the practice may still be viewed as unfair and unethical (Dennis, 2011). If the employer instead attempted to hack into or bypass the privacy settings without permission, then they may be liable under the SCA and other communication protections (Elzweig & Peeples, 2009).

SNS privacy is an area where it is more than likely acceptable for an employer to look at a person's public profile, one that is available for all to view. However, they may come into legal troubles when they attempt to access a profile that has had privacy settings to prevent everyone from viewing the site (Johnson, 2011). An employer could be potentially liable if they attempt to circumvent those privacy settings. Online communication via SNSs is often a permanent type of communication and the information from profiles is retrievable even after it has been deleted. Online communication does not have the same privacy protections that both a telephone conversation and a personal mailed letter have. Due to the permanency of the information it is important to procure privacy protections for SNS information (Clark & Roberts, 2010).

Potential Discrimination

Another major controversy of screening SNS profiles is the potential for discrimination. The majority of the United States has an employment-at-will doctrine which places the responsibility and power of employment in the hands of the employer (Clark & Roberts, 2010). Employers are able to choose who they want to hire, fire, and promote without direct limitations. However, with the emergence of the Civil Rights Act of 1964 and a variety of employment discrimination laws, employers must be more careful in their hiring practices to avoid discrimination lawsuits (Elzweig & Peeples, 2009). One way employers reduce their risk of discrimination lawsuits is by limiting their exposure to protected information.

Protected Information

SNS profiles provide a varying amount of protected information about applicants and employers who screen SNSs then have direct exposure to that information. An employer using SNS information for hiring decisions may either unintentionally or intentionally discriminate against applicants, causing adverse impact, due to the protected information that may be provided by SNSs (Bottomly, 2011; Brown & Vaughn, 2011; Davison, Maraist, & Bing, 2011; Dennis, 2011). “Adverse impact is the US legal doctrine which states that seemingly neutral practices may be legally challenged if they result in fewer minority members being hired” (Slovensky & Ross, 2012, p. 64). Information provided on SNSs could result in increased potential for adverse impact (Kluemper, Rosen, & Mossholder, 2012). The primary and most serious risk to an employer when they utilize SNS information for hiring decisions is a discrimination lawsuit due to the discovery of protected characteristics (e.g. race, religion, age, disability, and national origin) (Dennis, 2011; Slovensky & Ross, 2012; Sronce, 2011).

A considerable amount of the information that can be found on some SNS profiles, such as Facebook, is protected under various federal discrimination laws including Title VII of the Civil Rights Act of 1964, Americans with Disabilities Act, Age Discrimination in Employment Act, and a variety of other equal employment opportunity laws that cover the key areas of protected characteristics (Brown & Vaughn, 2011; Elzweig & Peeples, 2009). Other laws, such as state laws, may apply as well. The U.S. Equal Employment Opportunity Commission (EEOC) is responsible for the enforcement of the following federal laws that provide protections against employment discrimination. These protections are maintained in the hiring process (“Laws enforced by,” 2012).

Title VII of the Civil Rights Act of 1964

Title VII of the Civil Rights Act of 1964 prohibits employment discrimination based on race, color, sex, national origin, and religion (“Laws enforced by,” 2012). An employer may intentionally or unintentionally choose to not hire an individual due to this information. Besides the fact that some SNS profiles provide written information on sex, religion, and national origin, even a profile picture can provide information on estimated race, sex, and potentially even religion due to unique clothing or facial dress (Brown & Vaughn, 2011).

Americans with Disabilities Act Amendments Act of 2008

The Americans with Disabilities Act Amendments Act (ADAAA) of 2008 prohibits employment discrimination against those with a qualified disability. This includes both perceived and actual physical or mental impairment and the individual only has to be regarded as having the impairment to be protected (“Laws enforced by,” 2012). Substance addiction may qualify as a disability, yet nevertheless, empirical evidence has shown that alcohol-oriented SNS profiles decrease the likelihood that the individual would be hired (Bohnert & Ross, 2010). It has also been found that many employers may screen out applicants who display various alcohol-related habits and activities on their SNS profile. However, alcohol dependence is covered under the ADAAA. This means that the employer may be potentially discriminating against someone with a disability (Brown & Vaughn, 2011).

Age Discrimination in Employment Act of 1967

The Age Discrimination in Employment Act (ADEA) of 1967 prohibits discrimination against those who are 40 or older. With limited exceptions, an employer

who does not hire an applicant that is 40 or higher because of their age is discriminating against that individual (“Laws enforced by,” 2012). Some SNSs have age and even a birthdate listed on a user’s profile, unless they choose to omit that information.

Genetic Information Nondiscrimination Act of 2008

The Genetic Information Nondiscrimination Act (GINA) of 2008 prohibits discrimination on the basis of genetic information. Genetic information is any genetic test or evidence of a disease or disorder for both the individual and any blood-related family member up to a fourth-degree relative (“Laws enforced by,” 2012). This act was put in place as a result of employers not hiring an applicant because of a genetic disorder they may or may not get in the future, or one they have already so as to avoid further increase in health insurance costs to themselves. Because of the nature of SNSs, job applicants with a genetic disorder may have information on their profile relating to their disorder such as statuses about going to the doctor, medical care support page links, and other indicators. The most common risk when screening a SNS is discovering information about family medical history that may be hereditary in nature. For example, an applicant may post information about a parent who has or had cancer which implies an increased genetic risk of cancer for the applicant (Collins & Jackson, 2010). This information is protected by GINA, and an employer who discovers that information and refuses to hire the applicant due to their genetic disorder or predisposition would be held liable for discrimination (“Laws enforced by,” 2012). However, the law does state that only if an employer actively seeks the information on social networking sites would the search alone result in a violation of GINA. Genetic information that is found through inadvertent acquisition on a SNS would not result in a violation as long as that

information is not used to disqualify an applicant from being hired. (Collins & Jackson, 2010).

Pregnancy Discrimination Act of 1978

Finally, the Pregnancy Discrimination Act of 1978 prohibits sex discrimination on the basis of a pregnancy (“Laws enforced by,” 2012). In the case of hiring decisions, it is unlawful to refuse to hire an applicant solely based on the fact that the applicant is or may potentially become pregnant. Today, many expectant mothers will update family and friends on their SNS about their pregnancy, and some will even change their profile picture to their sonogram picture. This information is then readily available if an employer chooses to screen a SNS profile, which increases the risk they may discriminate against that pregnant applicant.

Fair Credit Reporting Act

Besides the laws that are covered by the EEOC, there are other laws that have implications for the practice of screening SNS profiles. The Fair Credit Reporting Act (FCRA) protects applicants from wrongful hiring decisions due to credit reporting information that runs the risk of being inaccurate or incomplete. It requires the employer to notify the applicant that they may conduct a credit background check. If the employer does not hire an applicant due to negative credit information, they must report the issue to the applicant so that they are able to follow up and attempt to correct any mistakes that may have occurred (Sronce, 2011). This potentially includes credit information that is found from a SNS profile. It is important to note that if an employer utilizes a third party to conduct the screening, the FCRA applies even if the screening is not specifically looking at credit information. This is often the case when an investigative consumer

report is obtained, which can provide information on the person's character, general reputation, personal characteristics, or mode of living. This information is often obtained through personal interviews with acquaintances of the person ("The fair credit," 2011).

Union Activity Rights

The Labor-Management Relations Act (Taft-Hartley Act) and the National Labor Relations Act (NLRA) also protects applicants that have pro-union opinions and activity from being discriminated against in the hiring process ("Are employees protected", 2011; Slovensky & Ross, 2012). Some information that is provided on a SNS profile may display pro-union opinions through pictures, statuses, or friends' posts. If an employer is anti-union and the applicant displays pro-union activity on a SNS profile, the employer may choose to not hire that applicant. However, this would be considered discrimination that is in violation of the Taft-Hartley Act. The NLRA goes further to state even a non-unionized person may be protected under the act if they display concerted activity regarding work conditions on a SNS profile. Concerted activity occurs if the discussion or postings are "engaged in, with, or on the authority of other employees, and not solely by and on behalf of the employee himself" ("Are employees protected", 2011, p.1). If an applicant displays concerted activity on their SNS, they are then protected by the NLRA and the National Labor Relations Board (NLRB) and a decision not to hire that applicant due to that information may be deemed discriminatory.

Social networking sites may provide much more protected information than employers should have. Employers screening SNS profiles may be receiving information that they otherwise would not choose to ask for in application materials or in an interview (Johnson, 2011; Kluemper, Rosen, & Mossholder, 2012; Sronce, 2011). Employers

could no longer use the defense that they were unaware of those attributes if it were proved that they readily accessed the information on the SNS (Dennis, 2011). It is important to note that these employment discrimination laws also apply to hiring firms and other employment agencies as well (Slovensky & Ross, 2012).

Potential for Adverse Impact

There is also the potential for adverse impact to occur when an applicant does not have a SNS profile. Because more is known about an applicant with an available SNS profile, those applicants without one may not be hired as often as someone who does have a SNS profile. This could be considered a practice that results in adverse impact if the majority of the applicants who do not have SNSs are minorities. If it is determined that this practice has adverse impact, then the company has a burden of proof to show that there is a legitimate business reason for the procedure in the selection of job candidates (Slovensky & Ross, 2012).

Unfortunately, it would be difficult to prove that an employer denied an applicant due to information found on a social networking site (Dennis, 2011). An employer is not required to disclose information about why they did not hire someone because of the employment-at-will doctrine (Brown & Vaughn, 2011). It is up to the applicant who felt that they may have been discriminated against, or had their privacy violated, to provide a legitimate claim against the employer.

Potential Solutions

Even though it may be difficult for an applicant to provide evidence that an employer did use SNS information to discriminate or violate privacy in the hiring process, an employer should be prepared. Researchers should continue studying and

validating the use of SNS information in the hiring process, because a lack of validation makes the practice difficult to defend legally. Several professional and governmental guidelines stress the importance of having a selection process that is validated, such as the Uniform Guidelines issued by the Equal Employment Opportunity Commission and supported by the Society of Industrial and Organizational Psychology (Brown & Vaughn, 2011).

Improve Legal Defensibility

Limited empirical support for SNS information's job relevance means that there is a limited legal basis for making a hiring decision using information gained from a SNS profile. The information from profile to profile and SNS to SNS is highly variable and lacks standardization, which is important for preventing legal ramifications. In order to increase the legal defensibility of using SNS information in hiring decisions, it is important for research to support a link between SNS information and predictors of job performance (Brown & Vaughn, 2011).

There are also a variety of procedures an employer can follow that may help prevent potential lawsuits in relation to screening SNS information as well as potentially reducing perceptions of unfairness. It is suggested that different SNS screening practices may result in different procedural justice perceptions. Most importantly, the employer should create a company policy on the practice of screening SNSs. The policy should state the legitimate business rationale for accessing that information (Bottomly, 2011; Waring & Buchanan, 2010). It should be clear enough to be easily understood and provide a process that is consistent regarding every applicant in order to remain as unbiased as possible (Brown & Vaughn, 2011; Elzweig & Peebles, 2009).

In order to protect themselves, employers should be consistent in their search practices and use verification processes for the information. This will help ensure the accuracy of the information they are using to make hiring decisions (Elzweig & Peeples, 2009; Johnson, 2011). Some suggest that the policy should include the following: to only view public information, never attempt to access information that is protected through privacy settings or passwords, and to avoid the use of false identities or deceptive actions to gain access to private information on a SNS (Johnson, 2011; Morin & Arce, 2011). It is recommended that screening SNS profiles should not go beyond what is available publicly (Waring & Buchanan, 2010).

It is also recommended that employers keep documentation of the hiring decision process (Elzweig & Peeples, 2009 Johnson, 2011). “Proof of legitimate rationale for rejecting applicants should be documented” (p.16) because it can help determine that the hiring decision was not based on discrimination due to knowledge of protected information (Waring & Buchanan, 2010). It is important for an employer to document hiring decisions in order to protect the company in case of potential lawsuits (Slovensky & Ross, 2012).

Use of Third-Party Reviewers

Another solution is to use a third-party reviewer to filter out protected information. As noted earlier, if a third-party reviewer is used there are other protections in place for the applicant through the Fair Credit Reporting Act (FCRA). A better solution might be the use of a neutral internal reviewer who has been trained to remove protected information before the employer views the SNS profile (Bottomly, 2011; Johnson, 2011; Kluemper, Rosen, & Mossholder, 2012). This would potentially help

protect the employer in discrimination lawsuits and reduce the FCRA implications (Johnson, 2011). Training applicant reviewers on potential privacy violation issues when screening SNS profiles is also recommended (Lanham, 2010).

Legislation Solutions

When it comes to technology, the law often lags behind and it is time for laws to regulate how employers use the information from SNSs. One legal solution that has been suggested is to expand the Fair Credit Reporting Act (FCRA). This solution however, is actually quite more complex and less feasible than one might think. Extending the FCRA to include SNS in the definition of a consumer reporting agent would be counterintuitive because the FCRA was created for a different purpose and to address a different range of information than for SNSs. Thus, it may be ill-equipped to regulate SNS information. Finally, the regulation of SNS information would be virtually unenforceable due to the nature of the SNS being ever changing and technology evolving at such a rapid rate (Sronce, 2011).

A better solution than expanding the FCRA may be to enact new legislation that addresses the issues of utilizing SNSs for hiring practices. Sronce (2011) suggested that employers should be required to inform applicants of potential screening of SNS information. This would hopefully help prevent potentially illegal hiring practices, such as discrimination, as well as relieving an applicant's suspicions that discrimination had occurred. Providing applicants with advanced notice of potential SNS screening may improve both actual and perceived fairness. It would hold the employer directly accountable and may even result in fewer employers screening SNS information. Even so, it will allow employers to screen the information without potentially using the

information in a discriminatory fashion. “There must be a law to ensure the appropriate use of SNSs, and a remedy in the event of inappropriate use” (p. 516).

Current Study

Because of the potential issues related to perceptions of fairness in the social networking site screening practices of an employer, this research study focused on those perceptions. As employers try to balance their legitimate business concerns with applicants' privacy concerns, fairness perceptions may have an impact on employers. However, the limited research available makes it unclear what types of practices result in lower fairness perceptions. This study sought to determine if different levels of privacy invasiveness and different levels of legitimate business concerns resulted in lower fairness perceptions.

Specifically, this study focused on the independent variables of privacy invasiveness and two types of legitimate business concerns: drug use and negative work comments. Privacy invasiveness is the amount of effort and depth taken in the screening process. There were three levels of privacy invasiveness included: viewing only a public SNS profile, "friending" the applicant, and requiring applicants' login information for their SNS profiles (Clark & Roberts, 2010; Dennis, 2011; Johnson, 2011; Lanham, 2010; Slovensky & Ross, 2012). Legitimate business concerns are information that has been found to screen out applicants from being hired because of the potential negative consequences that could manifest in the workplace (Brown & Vaughn, 2011). The drug use legitimate business concern included three levels: no drug use, marijuana use, and heroin addiction. The negative work comments legitimate business concern included three levels: no negative comments, ranting about employer, and threatening to bring a weapon to the workplace.

The purpose of this study was to examine the effects of privacy invasiveness and the two types of legitimate business concerns (i.e. drug use and negative work comments) on fairness perceptions. It was also of interest to determine if there was an interaction between the types of legitimate business concerns and privacy invasiveness on fairness perceptions. Due to the limited number of studies currently available, this study was largely exploratory.

Primary Research Focus

Hypothesis 1: There is an effect of privacy invasiveness such that higher invasion of privacy in the social networking screening process will relate to lower fairness perceptions.

Hypothesis 2: There is an effect of the two types of legitimate business concerns such that high legitimate business concerns found while screening social networking sites will relate to higher fairness perceptions.

Research Question 1: Is there an interaction between the levels of privacy invasiveness and finding legitimate business concerns that influences fairness perceptions of screening social networking sites?

It is believed that there is an interaction between privacy invasiveness and legitimate business concerns. However, due to the limited research available it is unclear what the interaction pattern may be and for this reason it has been posed as a research question. This is especially true for the situation where privacy invasiveness is high and the legitimate business concern is particularly alarming.

Additional Hypotheses

The above hypotheses and research questions were the primary focus of this study. However, there are additional hypotheses that were of interest as well. These hypotheses are largely in relation to demographics.

Hypothesis 3: There is an interaction between privacy invasiveness in the screening process and social networking site usage on fairness perceptions.

Hypothesis 4: There is an interaction between legitimate business concern found during the screening process and applicant screening experience on fairness perceptions.

CHAPTER II

Method

Participants

Participants of the study were obtained using the online application, Amazon Mechanical Turk (AMT). AMT is a crowdsourcing site that allows individual workers to choose tasks and/or jobs that they want to participate in (Buhrmester, Kwang, & Gosling, 2011). AMT offers a diverse subject pool that has been found to be representative of the general internet user population (Ipeirotis, 2010; Mason & Suri, 2012).

Participants were screened based on (a) passing an instrument manipulation check, and (b) using a reasonable amount of time to complete the survey. The manipulation check required participants to correctly answer three of four check items, and all did so. The reasonable time criterion screened out participants who took less than five minutes to complete the survey. Due to the number and depth of questions in the survey instrument, it is unlikely that a participant could have adequately read and answered all of the questions in that short time frame. This resulted in retaining 272 of the original 304 participants.

Demographic tables regarding the 272 participants are provided in Appendices B-G. Of these 272 participants, 47% were male and 53% were female. The mean age of participants was 33.20 with ages ranging from 18 to 72. The majority of the participants identified as being white or Caucasian, 78%. For job level, the largest percentage was for full-time employees with 39% identifying as such, followed by 21% being part-time employees and 17% unemployed but seeking employment.

Regarding prior social networking site usage, 95% had a social networking site account at the time of the survey. Of those participants, 87% had a Facebook account and 51% had a Twitter account. Participants were also asked the average time they spent on social networking sites with 70% saying they are on social networking sites daily. Of those participants who selected daily, the majority spend at least ten minutes and up to two hours on social networking sites every day. Participants also completed the Social Networking Site Intensity scale that was adapted from the Facebook Intensity Scale. This scale measures how personally connected the participant is with the social networking sites they use. The scale responses were scored on a 5-point Likert scale (1=strongly disagree, 5=strongly agree) (Ellison, Steinfeld, & Lampe, 2007). Cronbach's alpha of the six-item scale was .90. The mean social networking site intensity was 3.44, indicating that participants in general feel personally connected to social networking sites.

Participants were also asked about their experiences with screening applicants for jobs in their current or previous job positions. Of the 272 participants, 60 said they had assisted with or conducted job applicant screening processes during a hiring decision. Of those 60 participants, 42% stated that screening applicants in their job was rarely required, 37% stated it was occasionally required, and 22% stated it was frequently required. Lastly, participants were asked several questions relating to their personal experiences with social networking sites in the hiring process. An interesting result from this was that the vast majority of participants (97%) have not been required to disclose login information. Further results of applicant experiences can be found in Appendix G.

Design

The design of this study was a within-subjects factorial design. The general framework of this study was to examine the effects of the independent variables of privacy invasiveness and two types of legitimate business concerns on perceptions of fairness for screening social networking sites. There were three levels of privacy invasiveness included: viewing only a public SNS profile, “friending” the applicant, and requiring applicants’ login information for their SNS profiles. For legitimate business concerns, two types were used in this study: drug use and negative work comments. The drug use legitimate business concern included three levels: no drug use, marijuana use, and heroin addiction. Negative work comments also included three levels: no negative comments, ranting about employer, and threatening to bring a weapon to the workplace.

The two types of legitimate business concerns (i.e. drug use and negative work comments) and privacy invasiveness yielded two 3x3 ANOVAs. Each cell of the two 3x3 ANOVAs was created into a “scenario” for participants to rate on the dependent variable items for fairness perceptions. Fairness perceptions were measured by three different items: “This screening practice is fair to the applicant,” “The employer’s decision to do this screening practice is justified,” and “Not hiring an applicant based on this screening practice is justified.”

Drug Use Factorial Design

The first 3x3 ANOVA studied three levels of privacy invasiveness (low, medium, and high) used to obtain social networking site information with three levels of drug use (none, low, and high) as a legitimate business concern. The “none” level served as a control condition of not finding information that would indicate a legitimate business

concern. The privacy invasiveness levels were as follows: viewing only a public profile, friending the applicant, and requiring login information. The drug use levels were as follows: no indication of drug use, occasionally using marijuana, and severe addiction to heroin. The first 3x3 ANOVA is contained in Table 1.

Table 1. 3x3 Factorial Design for Privacy Invasiveness and Drug Use

		Legitimate Business Concern: Drug Use		
		None	Low	High
Privacy Invasiveness	Low	Public; No drugs	Public; Marijuana	Public; Heroin
	Medium	Friending; No drugs	Friending; Marijuana	Friending; Heroin
	High	Login Info; No drugs	Login Info; Marijuana	Login Info; Heroin

Negative Work Comments Factorial Design

The second 3x3 ANOVA studied the same three levels of privacy invasiveness (low, medium, and high) used to obtain social networking site information with three levels of negative work comments (none, low, and high) as a legitimate business concern. The negative work comments levels were as follows: no indication of negative work comments, ranting about current employer, and threatening complaints towards workplace. The second 3x3 ANOVA is contained in Table 2.

Table 2. 3x3 Factorial Design for Privacy Invasiveness and Negative Work Comments

		Legitimate Business Concern: Negative Work Comments		
		None	Low	High
Privacy Invasiveness	Low	Public; No negative comments	Public; Ranting comments	Public; Threatening comments
	Medium	Friending; No negative comments	Friending; Ranting comments	Friending; Threatening comments
	High	Login Info; No negative comments	Login Info; Ranting comments	Login Info; Threatening comments

Control Design

A control variable was used separately from the two 3x3 ANOVAs. This resulted in nineteen scenarios overall. The separate control variable was a general control that the employer did not do a screening of the social networking site. This variable was not included in the factorial design with privacy invasiveness and the two types of legitimate business concerns due to the inability to combine not screening a social networking site with finding legitimate business concerns while screening a social networking site. However, it was still of interest to the researchers to compare the fairness perceptions of not screening with the other levels of privacy invasiveness.

Procedure

The survey instrument was posted as a task on Amazon's Mechanical Turk website. Participants on AMT were able to choose to participate in the study by accepting the task. Only workers whose current location is in the United States were able to

participate. Once the participant selected the task, they were provided with a brief description of the study and a link to the online survey instrument hosted on Qualtrics.

In the online survey they were first asked to provide electronic consent to participate in the study. The survey began with participants rating the nineteen scenarios on three fairness perception items. The order of the scenarios was randomized to assist in reducing potential ordering effects. Participants were then asked to provide information on their current usage of social networking sites. Next, they were asked to disclose their experience with applicant screenings. Last, the participants were asked to provide demographic information of their age, gender, ethnicity, and job level. Participants were then given a survey code which they used in the Mechanical Turk site to verify their completion of the survey. Upon completion of the survey, participants received compensation of \$0.20. Compared to AMT's compensation standard, this compensation level is considerably higher than what is provided for the majority of tasks on AMT. Typically, it has been found that 25% of tasks pay \$0.01, 70% pay \$0.05 or less, and 90% pay less than \$0.10 (Ipeirotis, 2010).

Measures

Dependent Variables

Fairness Perceptions

Fairness perceptions of the screening practices were measured by using three separate items relating to fairness perceptions. At the time of the study it was not clear if these items could be combined into an overall fairness scale. The following three statements were rated on a 5-point Likert scale (1-strongly disagree, 5-strongly agree).

- “This screening practice is fair to the applicant”
- “The employer’s decision to do this screening practice is justified”
- “Not hiring an applicant based on this screening practice is justified”

Materials

Independent Variables

Privacy Invasiveness

Privacy invasiveness is described as the amount of effort the employer takes to find out information that would otherwise not be available to them. The levels of privacy invasiveness include: viewing only a public SNS profile, “friending” the applicant, and requiring applicants’ login information for their SNS profiles (Clark & Roberts, 2010; Dennis, 2011; Johnson, 2011; Lanham, 2010; Slovensky & Ross, 2012). These are considered to be in order of least invasive to most invasive.

- *Low*: The employer screened the applicant's public social networking profile
- *Medium*: The employer screened the applicant's social networking profile by “friending” the applicant
- *High*: The employer screened the applicant's social networking profile by requiring the applicant to provide their username and password information for the website

Legitimate Business Concerns

Legitimate business concerns are described as information that has been found to screen out applicants from being hired because of the potential negative consequences that could manifest in the workplace. This study focused on the two primary concerns of

drug use and negative work comments (Brown & Vaughn, 2011). Each one consisted of three qualitatively different levels (none, low and high) as indicated below.

- *Drug Use:*
 - None: “did not find information that indicated drug use”
 - Low: “found information that indicated the applicant occasionally used marijuana”
 - High: “found information that the applicant had a severe addiction to heroin”

- *Negative Work Comments:*
 - None: “did not find information that indicated negative work comments”
 - Low: “found information that the applicant often ranted about their current employer, sometimes with obscenities”
 - High: “found information that indicated the applicant was making threatening complaints to bring a weapon to their current workplace”

Control

The separate control condition was that no screening of social networking sites occurred. This variable was not included in the factorial design with privacy invasiveness and the two legitimate business concerns. Therefore, the control variable was its own scenario without combining with a legitimate business concern level: “The employer did not screen the applicant's social networking profile when making an employment decision.”

Scenarios

Scenarios were created by combining the identified levels of privacy invasiveness and legitimate business concerns. The unique combinations of the levels of privacy invasiveness and legitimate business concerns along with a separate control variable resulted in nineteen separate scenarios. For example: “The employer screened the applicant's social networking profile by requiring the applicant to provide their username and password information for the website and found information that indicated the applicant occasionally used marijuana.” This scenario included the high level of privacy invasiveness and the low level of illegal activity (legitimate business concern). The scenarios are provided in Appendix A (Q1-19).

Manipulation Checks

Four manipulation check items were created in order to determine response issues among participants. These manipulation check items were randomized into the scenario section. These items were questions that each participant should be able to correctly answer. The manipulation check items are provided in the Appendix A (Q20-23).

Demographic Variables

Social Networking Site Usage

Social networking site usage was measured using two separate items. The first item asked “How often do you visit a social networking site?” with five levels of usage ranging from once a month or less to daily visits. For those participants who stated they visit a SNS site daily, a second item asked “How much time in an average day do you spend on a social networking site?” with six levels of daily usage ranging from less than

ten minutes to more than three hours. The social networking site usage items are provided in Appendix A.

Social Networking Site Intensity

The Facebook Intensity scale was used to measure how personally connected the participant is with the social networking sites they use. The Cronbach's alpha has been reported at .83 (Ellison, Steinfeld, & Lampe, 2007). This scale was adapted to reflect social networking sites in general. The scale included six items and responses were scored on a 5-point Likert scale (1=strongly disagree, 5=strongly agree).

Applicant Screening Experience

Two items were used to capture the amount of experience participants have with screening applicants. The first item asked "Have you assisted with or conducted any type of job applicant screening processes during a hiring decision (e.g. background check, credit check, reference checks, social networking site screening, etc.)?" with responses being yes or no. The second item asked "How often does your current or previous job require you to screen job applicants during a hiring decision?" with three levels of screening experience: rarely required, occasionally required, and frequently required. The applicant screening experience items are provided in Appendix A (Q28-29).

Age, Gender, and Ethnicity

Participants were asked to self-report their age. They were also asked to self-report their gender as either female or male. Participants also self-reported their ethnicity using ethnic orientations from the Multigroup Ethnic Identity Measure (MEIM), which has reported a Cronbach's alpha of .80 (Phinney, 1992). Participants were able to choose

multiple responses for the ethnicity item. These items are provided in Appendix A (Q30-32).

Job Level

A measure of job level was used to differentiate between levels of employee positions. The item asked participants to select which job level(s) is most representative of their current job position. These items ranged from student to full-time employee options. Participants were able to choose multiple responses for this item. The job level item is provided in Appendix A (Q33).

Additional Background Information

Additional items were asked of participants in order to provide further descriptive information on the participants' experiences with social networking sites being used for employment reasons. These items are not a part of the hypotheses but are additional background information of interest. The additional background information items are provided in Appendix A (Q34).

CHAPTER III

Primary Results

Correlational Analyses

Spearman's correlations were conducted for several demographic items. A correlation matrix is provided in Appendix H. This matrix provides a summary of the relationships between the descriptive items from the survey.

Preliminary Analyses

Reliability analyses were conducted to determine if the three dependent variable items should remain separate items or whether any two or perhaps all three should be combined into a scale. Cronbach's alpha ranged from .89 to .93 for the legitimate business concern of Drug Use and from .85 to .94 for Negative Work Comments. For all of the scenarios, the reliability analyses showed that two of the three dependent variable items, "This screening practice is fair to the applicant" and "The employer's decision to do this screening practice is justified," were highly correlated. Cronbach's alpha was consistently higher with these two items combined than if left separately or if combined with the third item of "Not hiring an applicant based on this screening practice is justified." These results are provided in Appendix I. From these results, it was determined that the dependent variable items of "This screening practice is fair to the applicant" and "The employer's decision to do this screening practice is justified" would be combined into a scale of process fairness and the dependent variable item of "Not hiring an applicant based on this screening practice is justified" would remain as a rating of decision fairness.

Primary Analyses

To test the hypotheses and research questions of primary interest, a repeated-measures ANOVA analysis was conducted for privacy invasiveness separately with both types of legitimate business concern (i.e., Drug Use and Negative Work Comments) on both process fairness and decision fairness.

Process Fairness for Drug Use

A repeated-measures ANOVA was conducted for the legitimate business concern of Drug Use with the dependent measure of process fairness. Mauchly's Test of Sphericity indicated that the assumption of sphericity had been violated for the Privacy Invasiveness main effect, $\chi^2(2) = 44.44, p < .001$, and for the Privacy Invasiveness and Drug Use interaction, $\chi^2(9) = 31.22, p < .001$. Based on the Epsilon values, it was determined that the Huynh-Feldt adjustment would be appropriate for both the Privacy Invasiveness main effect ($\epsilon = .87$) and the Privacy Invasiveness and Drug Use interaction ($\epsilon = .96$). The assumption of sphericity was not violated for the Drug Use main effect, $\chi^2(2) = 2.27, p = .32$.

The Privacy Invasiveness main effect was statistically significant, $F(1.74, 444.12) = 154.90, p < .001$, partial $\eta^2 = 0.38$. The Drug Use main effect was statistically significant, $F(2, 512) = 9.20, p < .001$, partial $\eta^2 = 0.04$. The interaction effect of Privacy Invasiveness and Drug Use was not statistically significant, $F(3.84, 981.80) = 1.85, p = .12$, partial $\eta^2 = 0.01$.

Pairwise comparisons for the Privacy Invasiveness main effect revealed that all three levels of Privacy Invasiveness were significantly different from each other. Viewing a public profile was rated as higher in process fairness ($M = 3.01$) than friending an

applicant ($M = 2.68$), $p < .001$, as well as higher in process fairness than requiring login information ($M = 1.70$), $p < .001$. Process fairness of friending an applicant was also significantly different from process fairness of requiring login information, $p < .001$.

Pairwise comparisons for the Drug Use main effect revealed that finding no information that the applicant used drugs was rated lower in process fairness ($M = 2.46$) than finding information that the applicant used heroin ($M = 2.53$), $p < .05$. Also, finding information that the applicant used marijuana was rated lower in process fairness ($M = 2.40$) than finding information that the applicant used heroin, $p < .001$. Finding no information that the applicant used drugs and finding information that the applicant used marijuana were not significantly different from each other, $p = .18$. These results are provided below in Figure 1.

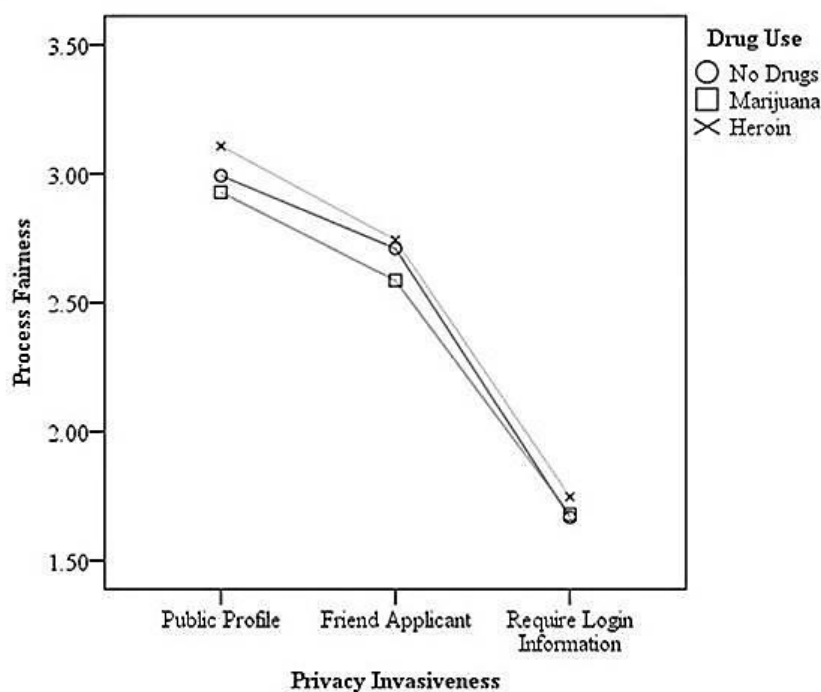


Figure 1. Process Fairness of Drug Use and Privacy Invasiveness

Decision Fairness for Drug Use

A repeated-measures ANOVA was conducted for the legitimate business concern of Drug Use with the dependent measure of decision fairness. Mauchly's Test of Sphericity indicated that the assumption of sphericity had been violated for the Privacy Invasiveness main effect, $\chi^2(2) = 85.69, p < .001$, the Drug Use main effect $\chi^2(2) = 29.28, p < .001$, and for the Privacy Invasiveness and Drug Use interaction, $\chi^2(9) = 30.71, p < .001$. Based on the Epsilon values, it was determined that the Huynh-Feldt adjustment would be appropriate for the Privacy Invasiveness main effect ($\epsilon = .78$), the Drug Use main effect ($\epsilon = .91$) and the Privacy Invasiveness and Drug Use interaction ($\epsilon = .96$).

The Privacy Invasiveness main effect was statistically significant, $F(1.57, 402.16) = 89.94, p < .001$, partial $\eta^2 = 0.26$. The Drug Use main effect was statistically significant, $F(1.82, 466.95) = 70.46, p < .001$, partial $\eta^2 = 0.22$. The interaction effect of Privacy Invasiveness and Drug Use was statistically significant, $F(3.84, 987.57) = 3.96, p < .01$, partial $\eta^2 = 0.02$.

Pairwise comparisons for the Privacy Invasiveness main effect revealed that all three levels of Privacy Invasiveness were significantly different from each other. Viewing a public profile was rated as higher in decision fairness ($M = 2.84$) than friending an applicant ($M = 2.60$), $p < .001$, as well as higher in decision fairness than requiring login information ($M = 1.95$), $p < .001$. Decision fairness of friending an applicant was also significantly different from decision fairness of requiring login information, $p < .001$.

Pairwise comparisons for the Drug Use main effect revealed that all levels of this legitimate business concern were significantly different from each other. Finding no

information that the applicant used drugs was rated lower in decision fairness ($M = 2.16$) than finding information that the applicant used marijuana ($M = 2.38$), $p < .001$, as well as finding information that the applicant used heroin ($M = 2.85$), $p < .001$. Also, finding information that the applicant used marijuana was rated significantly lower in decision fairness than finding information that the applicant used heroin, $p < .001$. These results are provided below in Figure 2.

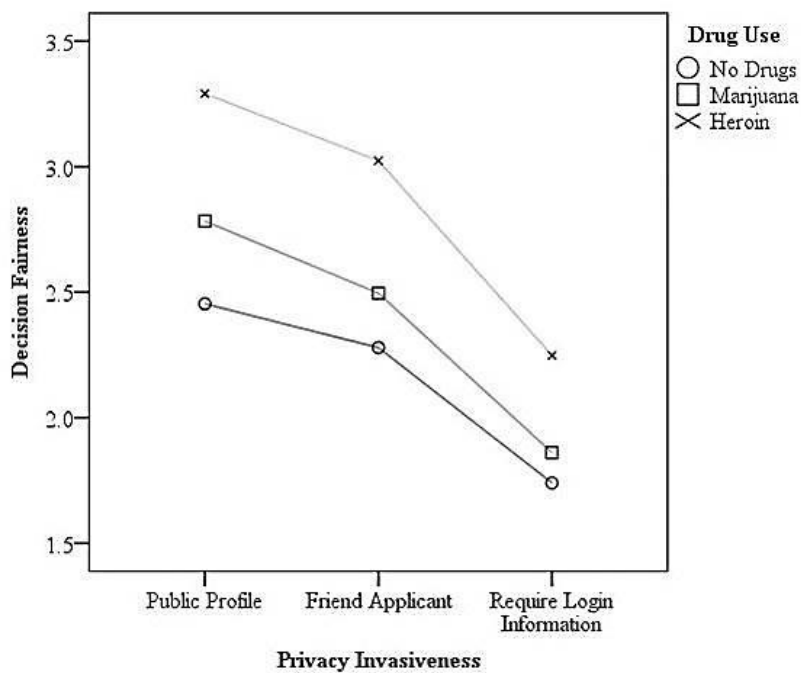


Figure 2. Decision Fairness of Drug Use and Privacy Invasiveness

Process Fairness for Negative Work Comments

A repeated-measures ANOVA was conducted for the legitimate business concern of Negative Work Comments with the dependent measure of process fairness. Mauchly's Test of Sphericity indicated that the assumption of sphericity had been violated for the Privacy Invasiveness main effect, $\chi^2(2) = 47.95, p < .001$, for the Negative Work Comments main effect, $\chi^2(2) = 71.39, p < .001$, and for the Privacy Invasiveness and Negative Work Comments interaction, $\chi^2(9) = 26.13, p < .01$. Based on the Epsilon values, it was determined that the Huynh-Feldt adjustment would be appropriate for the Privacy Invasiveness main effect ($\epsilon = .86$), the Negative Work Comments main effect ($\epsilon = .81$) and the Privacy Invasiveness and Negative Work Comments interaction ($\epsilon = .97$).

The Privacy Invasiveness main effect was statistically significant, $F(1.72, 439.72) = 172.20, p < .001$, partial $\eta^2 = 0.40$. The Negative Work Comments main effect was statistically significant, $F(1.62, 413.72) = 35.02, p < .001$, partial $\eta^2 = 0.12$. The interaction effect of Privacy Invasiveness and Negative Work Comments was statistically significant, $F(3.86, 989.23) = 3.90, p < .01$, partial $\eta^2 = 0.02$.

Pairwise comparisons for the Privacy Invasiveness main effect revealed that all three levels of Privacy Invasiveness were significant different from each other. Viewing a public profile was rated as higher in process fairness ($M = 3.06$) than friending an applicant ($M = 2.75$), $p < .001$, as well as higher in process fairness than requiring login information ($M = 1.75$), $p < .001$. Friending an applicant was also rated significantly different from requiring login information on process fairness, $p < .001$.

Pairwise comparisons for the Negative Work Comments main effect revealed that finding no information that the applicant made negative work comments was rated lower in process fairness ($M = 2.45$) than finding information that the applicant threatened to bring a weapon to the workplace ($M = 2.68$), $p < .001$. Also, finding information that the applicant occasionally ranted about their employer was rated lower in process fairness ($M = 2.43$) than finding information that the applicant threatened to bring a weapon to the workplace, $p < .001$. Finding no information that the applicant made negative work comments and finding information that the applicant occasionally ranted about their employer were not significantly different from each other on process fairness. These results are provided below in Figure 3.

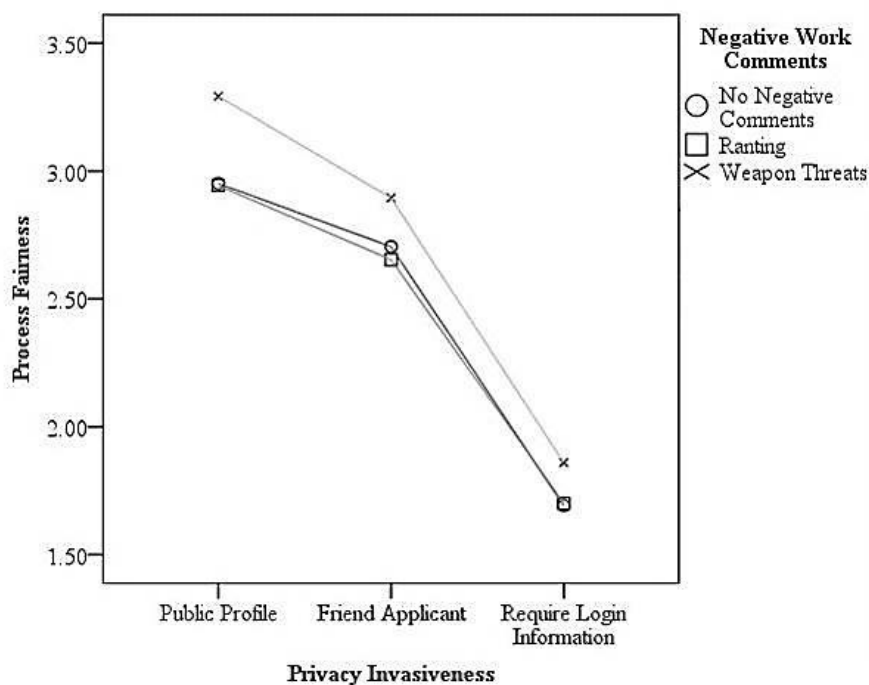


Figure 3. Process Fairness of Negative Work Comments and Privacy Invasiveness

Decision Fairness for Negative Work Comments

A repeated-measures ANOVA was conducted for the legitimate business concern of Negative Work Comments with the dependent measure of decision fairness. Mauchly's Test of Sphericity indicated that the assumption of sphericity had been violated for the Privacy Invasiveness main effect, $\chi^2(2) = 49.71, p < .001$, the Negative Work Comments main effect $\chi^2(2) = 53.17, p < .001$, and for the Privacy Invasiveness and Negative Work Comments interaction, $\chi^2(9) = 41.20, p < .001$. Based on the Epsilon values, it was determined that the Huynh-Feldt adjustment would be appropriate for the Privacy Invasiveness main effect ($\epsilon = .86$), the Negative Work Comments main effect ($\epsilon = .85$) and the Privacy and Negative Work Comments interaction ($\epsilon = .95$).

The Privacy Invasiveness main effect was statistically significant, $F(1.71, 449.18) = 98.00, p < .001$, partial $\eta^2 = 0.27$. The Negative Work Comments main effect was statistically significant, $F(1.70, 445.02) = 164.16, p < .001$, partial $\eta^2 = 0.385$. The interaction effect of Privacy Invasiveness and Negative Work Comments was statistically significant, $F(3.80, 994.84) = 4.00, p < .01$, partial $\eta^2 = 0.02$.

Pairwise comparisons for the Privacy Invasiveness main effect revealed that all three levels of Privacy Invasiveness were significant different from each other. Viewing a public profile was rated as higher in decision fairness ($M = 3.02$) than friending an applicant ($M = 2.79$), $p < .001$, as well as higher in decision fairness than requiring login information ($M = 2.12$), $p < .001$. Decision fairness of friending an applicant was also significantly different from decision fairness of requiring login information, $p < .001$.

Pairwise comparisons for the Negative Work Comments main effect revealed that all levels of this legitimate business concern were significantly different from each other

on decision fairness. Finding no information that the applicant made negative work comments was rated lower in decision fairness ($M = 2.19$) than finding information that the applicant occasionally ranted about their employer ($M = 2.41$), $p < .001$, as well as finding information that the applicant threatened to bring a weapon to the workplace ($M = 3.32$), $p < .001$. Also, finding information that the applicant occasionally ranted about their employer was rated significantly lower in decision fairness than finding information that the applicant threatened to bring a weapon to the workplace, $p < .001$. These results are provided below in Figure 4.

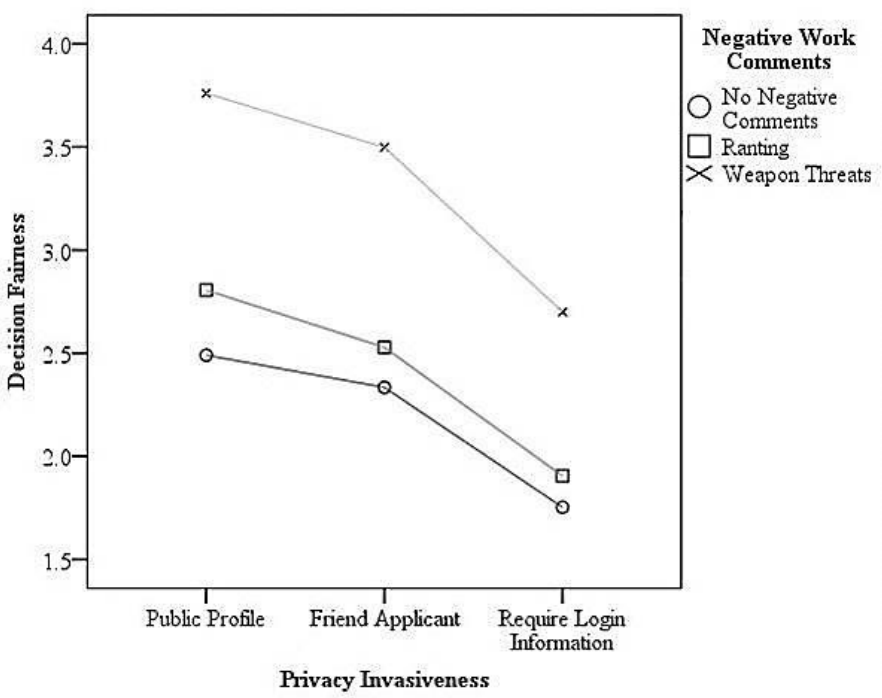


Figure 4. Decision Fairness of Negative Work Comments and Privacy Invasiveness

Primary Hypothesis Testing

Hypothesis 1: There is an effect of privacy invasiveness such that higher invasion of privacy in the social networking screening process will relate to lower fairness perceptions.

A significant main effect of Privacy Invasiveness on fairness perceptions would indicate support for this hypothesis. For process fairness and decision fairness, there were significant main effects of Privacy Invasiveness for both the Drug Use and the Negative Work Comments legitimate business concerns. Process fairness and decision fairness were rated higher when Privacy Invasiveness was low. Hypothesis 1 was supported in the results.

Hypothesis 2: There is an effect of legitimate business concern such that high legitimate business concerns found while screening social networking sites will relate to higher fairness perceptions.

A significant main effect of the two types of legitimate business concern on fairness perceptions would indicate support for this hypothesis. For the legitimate business concern of Drug Use, there were significant main effects for both process and decision fairness. Process and decision fairness were rated higher when Drug Use was high. For the legitimate business concern of Negative Work Comments, there were significant main effects for both process and decision fairness. Process and decision fairness were rated higher when Negative Work Comments was high. Hypothesis 2 was supported in the results.

Research Question 1: Is there an interaction between the levels of privacy invasiveness and finding legitimate business concerns that influences fairness perceptions of screening social networking sites?

The interaction effect of Privacy Invasiveness and Drug Use was not statistically significant for process fairness; however, it was statistically significant for decision fairness. The interaction effect of Privacy Invasiveness and Negative Work Comments was statistically significant for both process and decision fairness. However, the effect sizes for these results were small ($\eta^2 = 0.02$). These results provide some evidence of an interaction between Privacy Invasiveness and legitimate business concerns on process and decision fairness.

Additional Results

Control Condition Analyses

In addition to the above analyses, we explored the potential impact of a control condition, that the employer did not screen social networking sites, in comparison to the Privacy Invasiveness variable. In order to analyze the control condition, four repeated-measures mixed ANOVAs were conducted with the control condition being a between-subjects factor for both process and decision fairness. For the legitimate business concern of Drug Use, there was not a significant interaction of control with Privacy Invasiveness on process fairness, $F(14, 498) = 1.30, p = .20$, partial $\eta^2 = 0.04$; however, there was a significant interaction on decision fairness, $F(8, 506) = 2.32, p < .05$, partial $\eta^2 = 0.04$. For the legitimate business concern of Negative Work Comments, there was not a significant interaction of control with Privacy Invasiveness on process fairness,

$F(14, 498) = .95, p = .51, \text{partial } \eta^2 = 0.03$; or on decision fairness, $F(8, 516) = .98, p = .45, \text{partial } \eta^2 = 0.02$.

Social Networking Site Usage Analyses

Also explored was the potential impact of participants' social networking site usage with Privacy Invasiveness on both process and decision fairness. It was hypothesized that participants with more social networking site usage may have more privacy concerns and thus has lower fairness perceptions of the screening practices. The interest for these analyses was in the interaction of SNS usage and Privacy Invasiveness.

Two items of social networking site usage were analyzed. The first item asked "How often do you visit a social networking site?" with five levels of usage ranging from once a month or less to daily visits (Q27a, Appendix A). For those participants who stated they visit a SNS site daily, a second item asked "How much time in an average day do you spend on a social networking site?" with six levels of daily usage ranging from less than ten minutes to more than three hours (Q27b in Appendix A). Four repeated-measures mixed ANOVAs were conducted for each of the two social networking site usage items as between-subjects factors with the within-subject factor of Privacy Invasiveness for both process and decision fairness. None of the interaction results for social networking site usage with Privacy Invasiveness were significant.

Applicant Screening Experience Analyses

Also explored was the potential impact of participants' applicant screening experience with both types of legitimate business concerns, Drug Use and Negative Work Comments, on process and decision fairness. It was hypothesized that participants with experience in screening applicants during the hiring process would be more sensitive to

legitimate business concerns and thus would have higher fairness perceptions. The interest for these analyses was in the interaction of applicant screening experience and the two types of legitimate business concerns.

Two items were used to capture the amount of experience participants have with screening applicants. The first item asked “Have you assisted with or conducted any type of job applicant screening processes during a hiring decision (e.g. background check, credit check, reference checks, social networking site screening, etc.)?” with responses being yes or no (Q28, Appendix A). For participants who said “yes” they have conducted applicant screenings, a second item asked “How often does your current or previous job require you to screen job applicants during a hiring decision?” with three levels of screening experience: rarely required, occasionally required, and frequently required (Q29, Appendix A). Four repeated-measures mixed ANOVAs were conducted for each of the two applicant screening items as between-subjects factors with each type of legitimate business concern as within-subject factors for both process and decision fairness. None of the interaction results for applicant screening experience with the two types of legitimate business concerns were significant.

Additional Hypothesis Testing

Hypothesis 3: There is an interaction between privacy invasiveness in the screening process and social networking site usage on fairness perceptions.

It was hypothesized that high social networking site users have more privacy concerns and thus have lower fairness perceptions than those who are low social networking site users. A significant interaction was not found between both measures of

social networking site usage and Privacy Invasiveness on fairness perceptions.

Hypothesis 3 was not supported in the results.

Hypothesis 4: There is an interaction between legitimate business concern found during the screening process and applicant screening experience on fairness perceptions.

It was hypothesized that participants with applicant screening experience are more sensitive to legitimate business concerns and thus have higher fairness perceptions than those who do not have applicant screening experience. A significant interaction was not found between both measures of applicant screening experience and Drug Use or Negative Work Comments on fairness perceptions. Hypothesis 4 was not supported in the results.

CHAPTER IV

Discussion

The results of this study supported the hypotheses that the level of privacy invasiveness used by the employer and the level of the legitimate business concern found during the screening influence fairness perceptions. The privacy invasiveness main effect was consistent across both types of legitimate business concerns and indicated that higher privacy invasiveness resulted in both lower process and decision fairness. This result has implications for employers that choose to conduct social networking site screenings, especially practices that are seen as more invasive. Practices such as friending an applicant, trying to circumvent privacy settings, and requiring login information have the potential to be seen as low in fairness perceptions. Previous research indicates that these fairness perceptions could influence applicant reactions such as test taking motivation, organizational attraction and organizational intentions (e.g. rejecting an offer and discouraging others to apply for a job) (Bauer et al., 2006; Slovinsky & Ross, 2012). Employers practicing more invasive screening procedures could be negatively impacted by losing key talent in the selection process due to these fairness perceptions. It would be beneficial for future research to study these measures of applicant reactions as well as litigation intentions, the perception of whether or not the practice would result in an applicant to sue the employer (Bauer et al., 2001). With new state laws being passed in relation to these practices and the potential for protection under the Stored Communications Act, certain screening practices may not only be seen as unfair but could be illegal. Determining what types of screening practices may lead to higher litigation intentions could assist employers in choosing future screening practices to

reduce the chance of litigation. These applicant reaction measures could provide further information on how employers' screening practices can influence perceptions and how it might impact the company.

The main effects of both drug use and negative work comments indicated that less serious levels of legitimate business concerns resulted in both lower process and decision fairness. This indicates that social networking site screening practices may be seen as more fair when the legitimate business concern is high. However, these fairness perceptions in relation to legitimate business concerns may not align with what the law states an employer can practice in the hiring process. For instance, when drug use was high (i.e. severe addiction to heroin) results showed higher process and decision fairness for employers to screen social networking sites and not hire an applicant based on that information. This may indicate that employers also believe it is justified to screen out individuals with evidence of drug use on their social networking sites. In fact, previous research has found that even applicants who display various alcohol-related habits and activities on their profile are less likely to be hired (Bohnert & Ross, 2010). However, alcohol dependence and other addictions such as heroin use are covered under the Americans with Disabilities Act Amendments Act of 2008. This means that the employer may be discriminating against someone with a disability and therefore engaging in an illegal practice (Brown & Vaughn, 2011). Although fairness perceptions are sympathetic to this type of legitimate business concern, it does not align with the legal requirements held to employers.

The results of the negative work comments' main effects indicate that lower levels of this legitimate business concern result in lower fairness perceptions. In fact, the

pattern of results for negative work comments was more pronounced than the pattern of results for drug use. When the negative work comments level was potentially threatening, process and decision fairness were rated much higher in comparison to the lower levels. This indicates that concern for workplace safety may result in higher fairness perceptions when screening social networking sites.

Results of the interaction effect between the two types of legitimate business concerns and privacy invasiveness were mixed. For the drug use legitimate business concern, the interaction with privacy invasiveness on process fairness was not significant. This non-significance is potentially due to the fact that participants did not rate “no drug use” and “marijuana use” significantly different from each other on process fairness. This indicates that “no drug use” and “marijuana use” were viewed similarly on whether or not the screening practice was fair or justified. Although “severe addiction to heroin” was rated significantly different from “no drug use” and “marijuana use,” the process fairness perceptions were not drastic (i.e. around a tenth of a point). Because process fairness focuses on the actual screening practice and not what was found as a result of the process, the fact that this interaction was not significant is actually a reasonable result. The remaining interaction effects of drug use on decision fairness and negative work comments on process and decision fairness were significant. In general, fairness perceptions were lowered as the legitimate business concerns decreased and privacy invasiveness increased. The fact that the interaction of negative work comments and privacy invasiveness on process fairness was significant is an interesting finding. This indicates that participants were partly reacting to what was found at the end of the screening process (i.e. weapon threat) rather than the actual process alone when rating

process fairness. In the case of extreme behaviors such as threatening to bring a weapon to the workplace, it is possible that the participants were more influenced by an “ends justify the means” mentality. This was further demonstrated by the fact that the interactions on decision fairness were significant. This result along with the main effect of negative work comments indicates that extreme behaviors such as threatening to bring a weapon to the workplace may be information that participants, and potentially employers alike, view as worth taking the risks to find.

The results of the main effects and interactions suggest that employers should be cognizant of the way in which their screening practices may be perceived by applicants and whether or not they could be potentially illegal. As more employers are screening social networking sites for hiring purposes it becomes more imperative that they attempt to balance applicants’ privacy expectations with the legitimate business concerns that an employer is entitled to for hiring decisions (Dennis, 2011). There have been several proposed solutions to attempt this balance and to potentially reduce litigation against employers. One simple step employers could take is to become transparent about their practices and inform their applicants of the screening. This could potentially increase fairness perceptions of the practice. Future researchers may want to explore this further and provide empirical evidence on how this transparency could influence fairness perceptions and other applicant reactions. Finally, it is imperative that employers remain informed on the laws that impact these practices and ensure they are not exposing themselves to potential legal ramifications.

This research study was largely exploratory due to the limited research available on the subject. Both the scenarios used and the dependent variables were constructed by

the researchers and further analyses of these measures is warranted. A within-subjects, repeated measures design was used for this study. The primary purpose of using the within-subjects design was to increase power. The within-subjects design would also reduce the chances of individual differences skewing the fairness perception results. However, this design has the potential limitation of carryover effects in which the first scenarios influence ratings of the following scenarios. To reduce potential ordering effects, these scenarios were counterbalanced by using pure randomization of the scenarios in the online survey. Future researchers may want to consider utilizing a between-subjects approach to supplement these results.

Although the current literature on Amazon Mechanical Turk suggests that the users are representative of the general internet user population and is a reliable source for social research, there were still some concerns about this source (Mason & Suri, 2012; Ipeirotis, 2010). For this study, several participants had a survey duration that was less than five minutes in length and due to concerns of reliable responses were removed from the final data set. Four manipulation checks were also randomized within the scenarios to determine if participants were not reliable responders. The manipulation checks did not require further removal of participants. It is possible that because the manipulation checks were structured differently (i.e. true/false response) from the scenarios (i.e. Likert scale) that respondents may have been more aware of these checks when they occurred. Future researchers may want to structure their manipulation checks more similarly in format to the scenarios. Also, it is recommended that future researchers replicate this study using other populations such as in higher education, industry, and other internet settings. It may also be useful to have a greater representation of participants who have

been required to provide login information. Replication of this study with other populations would increase the generalizability of these results.

Future researchers should also include other legitimate business concerns in their research to determine if they also have an influence on fairness perceptions in social networking site screening. Other legitimate business concerns that have been considered in the literature include risqué or inappropriate behavior, falsified information on resumes, lack of required job-relevant skills, and poor communication skills. It would also be valuable to research further the influence of workplace safety concerns on fairness perceptions. Lastly, a limitation of this study is the issue of common method variance. This method bias potentially distorts the observed relationship by inflating the variance. For future research, it would be beneficial to consider alternative methods to reduce common method variance.

References

- Ahearn, T. (2012, August 7). *Illinois law prevents employers from demanding social network passwords from employees and job candidates*. Retrieved from <http://www.esrcheck.com/wordpress/2012/08/07/illinois-law-prevents-employers-from-demanding-social-network-passwords-from-employees-and-job-candidates/>
- Ahearn, T. (2012, October 2). *California social media privacy law ab 1844 prohibits employers from demanding usernames and passwords from applicants and employees*. Retrieved from <http://www.esrcheck.com/wordpress/2012/10/02/california-social-media-privacy-law-ab-1844-prohibits-employers-from-demanding-usernames-and-passwords-from-applicants-and-employees/>
- Are employees protected when using social media? (2011, December 06). *Honigman Alert*. Retrieved from <http://www.honigman.com>
- Bauer, T.N., Truxillo, D.M., Sanchez, F.J., Craig, J.M., Ferrara, P., & Campion, M.A. (2001). Applicant reactions to selection: Development of the selection procedural justice scale (SPJS). *Personnel Psychology*, *54*, 387–419.
- Bauer, T., Truxillo, D., Tucker, J., Weathers, V., Bertolino, M., Erdogan, B., & Campion, M. (2006). Selection in the information age: The impact of privacy concerns and computer experience on applicant reactions. *Journal of Management*, *32*(5), 601-621. doi: 10.1177/0149206306289829
- Bohnert, D., & Ross, W. H. (2010). The influence of social networking web sites on the evaluation of job candidates. *Cyberpsychology, Behavior, and Social Networking*, *13*(3), 341-347. doi: 10.1089/cyber.2009.0193

- Bottomly, L. G. (2011, July). *Social media: New opportunities and headaches*. Paper presented at Employment law seminar. doi: 1023255/3/LGB/000100-0233
- 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, 219-225. doi: 10.1007/s10869-011-9221-x
- Buhrmester, M., Kwang, T., & Gosling, S. D. (2011). Amazon's mechanical turk: A new source of inexpensive, yet high-quality data?. *Perspectives on Psychological Science*, 6(1), 3-5. doi: 10.1177/1745691610393980
- Clark, L. A., & Roberts, S. J. (2010). Employer's use of social networking sites: a socially irresponsible practice. *Journal of Business Ethics*, 95, 507-525. doi: 10.1007/s10551-010-0436-y
- Collins, E. M., & Jackson, R. M. (2010). Complying with the genetic information nondiscrimination act: Acquisition, storage, disclosure, and social media . *Employment Law Alert*, Retrieved from http://www.nixonpeabody.com/files/Employment_Law_Alert_EEOC_11_11_2010.pdf
- Davison, H. K., Maraist, C., & Bing, M. N. (2011). Friend or foe? The promise and pitfalls of using social networking sites for h.r. decisions. *Journal of Business and Psychology*, 26, 153-159. doi: 10.1007/s10869-011-9215-8
- Dennis, C. M. (2011). Legal implications of employee social media use. *Massachusetts Law Review*, 93(4), 380-395. Retrieved from <http://www.massbar.org/publications/massachusetts-law-review/2011/vol-93-no-4/legal-implications-of-employee-social-media-use>

- Egan, E. (2012, March 23). [Web log message]. Retrieved from <https://www.facebook.com/notes/facebook-and-privacy/protecting-your-passwords-and-your-privacy/326598317390057>
- Ellison, N. B., Steinfeld, 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, 1143-1168. doi: 10.1111/j.1083-6101.2007.00367.x
- Elzweig, B., & Peeples, D. K. (2009). Using social networking web sites in hiring and retention decisions. *Advanced Management Journal*, (Autumn), 27-35.
- Federal Trade Commission, (2011). *The fair credit reporting act*. Retrieved from website: <http://www.ftc.gov/os/statutes/031224fcra.pdf>
- Greenberg, P. (2013, April 22). *Employer access to social media usernames and passwords 2013*. Retrieved from <http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords-2013.aspx>
- Ipeirotis, P. G. (2010). Analyzing the amazon mechanical turk marketplace. *XRDS: Crossroads*, 17(2), 16-21. doi: 10.1145/1869086.1869094
- Johnson, E. M. (2011, September). *Social media and labor & employment law: Job applications & background checks, employee misconduct, ethical considerations*. Paper presented at 2011 annual association law symposium, Washington, D.C.
- Katz v. United States. 389 U.S. 347. (1967).
- Kluemper, D. H., & Rosen, P. A. (2009). Future employment selection methods: Evaluating social networking web sites. *Journal of Managerial Psychology*, 24(6), 567-580. doi: 10.1108/02683940910974134

- Kluemper, D. H., Rosen, P. A., & Mossholder, K. W. (2012). Social networking websites, personality ratings, and the organizational context: More than meets the eye?. *Journal of Applied Social Psychology*, 1-30. doi: 10.1111/j.1559-1816.2011.00881.x
- Lanham, J. R. (2010). Social media and the workplace. *Employment Law Commentary*, 22(1), 1-7. Retrieved from <http://www.mofo.com/social-media-and-the-workplace-02-01-2010/>
- Laws enforced by the EEOC*. (2012). Retrieved from <http://www.eeoc.gov/laws/statutes/index.cfm>
- Library of Congress, (2012). *S.3075 password protection act of 2012*. Retrieved from website: <http://beta.congress.gov/bill/112th-congress/senate-bill/3074>
- Martucci, W. C., & Shankland, R. J. (2012). New laws prohibiting employers from requiring employees to provide access to social-networking sites. *Employment Relations Today*, 79-85. doi: 10.1002/ert
- Mason, W., & Suri, S. (2012). Conducting behavior research on amazon's mechanical turk. *Behavioral Research Methods*, 44, 1-23. doi: 10.3758/s13428-011-0124-6
- Morin, P., & Arce, E. T. (2011). Social media: Balancing the rights of employers and employees. *Western City*, Retrieved from <http://www.westerncity.com>
- Phinney, J. (1992). The Multigroup Ethnic Identity Measure: A new scale for use with adolescents and young adults from diverse groups. *Journal of Adolescent Research*, 7, 156-176.
- Pietrylo v. Hillstone Restaurant Group. Docket No. 2:06-cv-05754. (2008).

- Slovensky, R., & Ross, W. H. (2012). Should human resource managers use social media to screen job applicants? Managerial and legal issues in the usa. *info*, *14*(1), 55-69. doi: 10.1108/14636691211196941
- Sronce, C. R. (2011). The references of the twenty-first century: Regulating employers' use of social networking sites as an applicant screening tool. *Southern Illinois University Law Journal*, *35*(3), 499-516.
- Truxillo, D. M., & Bauer, T. N. (1999). Applicant reactions to test score banding in entry level and promotional contexts. *Journal of Applied Psychology*, *84*, 322-340.
- Waring, R. L., & Buchanan, F. R. (2010). Social networking web sites: The legal and ethical aspects of pre-employment screening and employee surveillance. *Journal of Human Resources Education*, *4*(2), 14-23.

APPENDICES

Appendix A: Survey Instrument

Informed Consent

Please read the following before continuing with the survey.

The purpose of this research project is to study how fair people believe it is for employers to use social networking site (e.g. Facebook or Twitter) information for hiring decisions of job applicants. You will be asked to complete an online survey that will take approximately 10-30 minutes. This is a research project being conducted by Kimberly Kluesner, an Industrial/Organizational Psychology Master's candidate at Middle Tennessee State University, as part of a thesis requirement. This research has been reviewed according to Middle Tennessee State University IRB procedures for research involving human participants.

Your participation in this research study is completely voluntary and you may withdraw at any time. Your responses will be kept confidential. The results of this study will be used for scholarly purposes only and may be shared with Middle Tennessee State University representatives.

If you have any questions about the research study, please contact Kimberly Kluesner via email at kk3b@mtmail.mtsu.edu.

ELECTRONIC CONSENT:

Clicking on the next button below indicates that:

- you have read the above information
- you voluntarily agree to participate

If you do not wish to participate in the research study, please decline participation by closing out of the survey.

Scenarios

For the following scenarios, please select your level of agreement with each statement.

Rating Matrix (for each scenario):

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
The screening practice is fair to the applicant.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The employer's decision to do this screening practice is justified.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Not hiring an applicant based on this screening practice is justified.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Q1 The employer did not screen the applicant's social networking profile when making an employment decision.

Q2 The employer screened the applicant's public social networking profile and found information that indicated the applicant occasionally used marijuana.

Q3 The employer screened the applicant's public social networking profile and found information that the applicant had a severe addiction to heroin.

Q4 The employer screened the applicant's public social networking profile and did not find information that indicated drug use.

Q5 The employer screened the applicant's public social networking profile and found information that the applicant often ranted about their current employer, sometimes using obscenities.

Q6 The employer screened the applicant's public social networking profile and found information that indicated the applicant was making threatening complaints to bring a weapon to their current workplace.

Q7 The employer screened the applicant's public social networking profile and did not find information that indicated negative work comments.

Q8 The employer screened the applicant's social networking profile by “friending” the applicant and found information that indicated the applicant occasionally used marijuana.

Q9 The employer screened the applicant's social networking profile by “friending” the applicant and found information that the applicant had a severe addiction to heroin.

Q10 The employer screened the applicant's social networking profile by “friending” the applicant and did not find information that indicated drug use.

Q11 The employer screened the applicant's social networking profile by “friending” the applicant and found information that the applicant often ranted about their current employer, sometimes using obscenities.

Q12 The employer screened the applicant's social networking profile by “friending” the applicant and found information that indicated the applicant was making threatening complaints to bring a weapon to their current workplace.

Q13 The employer screened the applicant's social networking profile by “friending” the applicant and did not find information that indicated negative work comments.

Q14 The employer screened the applicant's social networking profile by requiring the applicant to provide their user-name and password and found information that indicated the applicant occasionally used marijuana.

Q15 The employer screened the applicant's social networking profile by requiring the applicant to provide their user-name and password and found information that the applicant had a severe addiction to heroin.

Q16 The employer screened the applicant's social networking profile by requiring the applicant to provide their user-name and password and did not find information that indicated drug use.

Q17 The employer screened the applicant's social networking profile by requiring the applicant to provide their user-name and password and found information that the applicant often ranted about their current employer, sometimes using obscenities.

Q18 The employer screened the applicant's social networking profile by requiring the applicant to provide their user-name and password and found information that indicated the applicant was making threatening complaints to bring a weapon to their current workplace.

Q19 The employer screened the applicant's social networking profile by requiring the applicant to provide their user-name and password and did not find information that indicated negative work comments.

Manipulation Checks

Q20 The year in which you are taking this survey is 2011.

- True
- False

Q21 The country you currently reside in is the United States of America.

True

False

Q22 This is a survey about fairness perceptions of employers using social networking site (e.g. Facebook) information to screen out applicants from the hiring process.

True

False

Q23 This survey is being conducted using Amazon Mechanical Turk.

True

False

Social Networking Site Usage

Q24 Do you currently have a social networking site account (e.g. Facebook, Twitter, LinkedIn, etc.)?

Yes

No

If No Is Selected, Then Skip To End of Block

Q25 Which of the following social networking sites do you currently have an account with? (please check all that apply)

Facebook

Twitter

LinkedIn

Myspace

Other _____

Q26 Please select your level of agreement for the following statements regarding your social networking site usage.

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
Social networking sites are part of my everyday activity.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I am proud to tell people that I am on social networking sites.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Social networking sites have become part of my daily routine.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I feel out of touch when I have not logged onto a social networking site for awhile.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I feel I am part of the social networking site communities.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I would be sorry if social networking sites were shut down.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Q27a How often do you visit a social networking site?

- Once a month or less
- A few times a month

- Once a week
- A few times a week
- Daily

Q27b How much time in an average day do you spend on a social networking site?

- Less than 10 minutes
- 10-30 minutes
- 31-60 minutes
- 1-2 hours
- 2-3 hours
- More than 3 hours

Applicant Screening Experience

Q28 Have you assisted with or conducted any type of job applicant screening processes during a hiring decision (e.g. background check, credit check, reference checks, social networking site screening, etc.)?

- Yes
- No

If No Is Selected, Then Skip To End of Block

Q29 How often does your current or previous job require you to screen job applicants during a hiring decision?

- Applicant screening is rarely required in my current/previous job
- Applicant screening is occasionally required in my current/previous job
- Applicant screening is frequently required in my current/previous job

Demographics

Q30 What is your age?

Q31 What is your gender?

- Male
- Female

Q32 What is your ethnicity?

- White, Caucasian, Anglo, European American; not Hispanic
- Black or African American
- Asian or Asian American, including Chinese, Japanese, and others
- Hispanic or Latino, including Mexican American, Central American, and others
- American Indian/Native American
- Mixed; parents from two different ethnic groups
- Other _____

Q33 Please select which job level(s) is most representative of your current job position.

- Unemployed, seeking employment
- Unemployed, not seeking employment
- Part-Time Employee
- Full-Time Employee
- Student

Q34 The following are items asking about your experience with social networking sites.

Please select the appropriate response for each item.

	Yes	No	Not Sure
Have you been asked to disclose your login information by an employer?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Have you been asked to disclose your browser history by an employer?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Do you believe you have been denied a job based on information an employer found on your social networking site profile(s)?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Do you believe a friend or family member has been denied a job based on information an employer found on their social networking site profile(s)?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Do you believe that you have received a job offer because of your LinkedIn profile?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Do you have more than one Facebook page (e.g. profile for work and a private profile for family and friends only)?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Survey Code

To receive compensation enter the following survey code in Mechanical Turk: 05112013

Appendix B: Ethnicity

	Frequency	Percent
White	219	78
African American	17	6
Asian	17	6
Hispanic/Latino	14	5
Native American	5	2
Mixed Ethnicity	8	3
Other	1	4
Total	281	

Note. Multiple responses were permitted.

Appendix C: Job Level

	Frequency	Percent
Unemployed, seeking employment	50	17
Unemployed, not seeking employment	27	9
Part-time employee	61	21
Full-time employee	114	39
Student	43	15
Total	295	

Note. Multiple responses were permitted.

Appendix D: Social Networking Site Accounts

	Frequency	Percent
Facebook	237	87
Twitter	138	51
LinkedIn	110	40
MySpace	50	18
Other	28	10

Note. Multiple responses were permitted.

Appendix E: Average Time Spent on Social Networking Sites

	Frequency	Percent
Once a month or less	14	5
A few times a month	15	6
Once a week	12	5
A few times a week	36	14
Daily	180	70

Appendix F: Average Time Spent on Social Networking Sites Daily

	Frequency	Percent
Less than 10 minutes	14	8
10-30 minutes	47	26
31-60 minutes	40	22
1-2 hours	35	19
2-3 hours	16	9
More than 3 hours	28	16

Appendix G: Applicant Experiences

	Frequency	Percent
Asked to disclose login information		
Yes	8	3
No	263	97
Not sure	1	0.4
Asked to disclose browser history		
Yes	5	2
No	265	98
Not sure	1	0.4
Denied a job based on social networking site profile		
Yes	4	2
No	240	88
Not Sure	28	10
Friend or family member has been denied based on social networking profile		
Yes	32	12
No	188	69
Not Sure	52	19
Received job offer because of LinkedIn profile		
Yes	24	9
No	236	96
Not Sure	12	4
More than one Facebook page		
Yes	34	13
No	236	87
Not Sure	2	1

Appendix H: Correlations

	Social Networking Site Frequency	Daily Social Networking Site Frequency	Job Applicant Screening Experience	Job Applicant Screening Frequency	Age	Gender ^a
Job Applicant Screening Experience	.107	.026				
Job Applicant Screening Frequency	.107	-.036				
Age	-.122	-.118	-.138*	.081		
Gender ^a	.061	.149*	-.056	.044	.059	
Social Networking Site Intensity	.648**	.432**	.039	.200	-.067	.148*

Note.

****.** Correlation is significant at the 0.01 level (2-tailed).

*****. Correlation is significant at the 0.05 level (2-tailed).

^aFor Gender, male was coded as 1 and female was coded as 2.

Appendix I: Scale Reliability

Drug Scenario Scales Reliability

	Cronbach's Alpha	Cronbach's Alpha if "Not hiring" Item Excluded
Public Profile, Marijuana	.939	.964
Public Profile, Heroin	.930	.965
Public Profile, No Drug	.893	.959
Friend Applicant, Marijuana	.934	.953
Friend Applicant, Heroin	.922	.947
Friend Applicant, No Drug	.930	.965
Require Login, Marijuana	.930	.939
Require Login, Heroin	.898	.944
Require Login, No Drug	.908	.935

Negative Work Comments Scenario Scales Reliability

	Cronbach's Alpha	Cronbach's Alpha if "Not hiring" Item Excluded
Public Profile, Ranting	.937	.957
Public Profile, Weapon Threats	.922	.947
Public Profile, No Negative Comments	.899	.965
Friend Applicant, Ranting	.940	.965
Friend Applicant, Weapon Threats	.899	.935
Friend Applicant, No Negative Comments	.893	.951
Require Login, Ranting	.924	.934
Require Login, Weapon Threats	.849	.927
Require Login, No Negative Comments	.889	.949

Appendix J: IRB Approval

February 4, 2013

Kimberly Kluesner, Patrick McCarthy, Ph.D., J.D.
Department of Industrial and Organizational Psychology
kk3b@mtmail.mtsu.edu, Patrick.Mccarthy@mtsu.edu

Protocol Title: "Fairness Perceptions of Screening Social Networking Sites for Hiring Decisions"

Protocol Number: 13-191

Dear Investigator(s),

The exemption is pursuant to 45 CFR 46.101(b) (2). This is because the research being conducted involves the use of educational tests, survey procedures, interview procedures or observation of public behavior.

You will need to submit an end-of-project report to the Compliance Office upon completion of your research. Complete research means that you have finished collecting data and you are ready to submit your thesis and/or publish your findings. Should you not finish your research within the three (3) year period, you must submit a Progress Report and request a continuation prior to the expiration date. Please allow time for review and requested revisions. Your study expires on **February 4, 2016**.

Any change to the protocol must be submitted to the IRB before implementing this change. According to MTSU Policy, a researcher is defined as anyone who works with data or has contact with participants. Anyone meeting this definition needs to be listed on the protocol and needs to provide a certificate of training to the Office of Compliance. **If you add researchers to an approved project, please forward an updated list of researchers and their certificates of training to the Office of Compliance before they begin to work on the project.** Once your research is completed, please send us a copy of the final report questionnaire to the Office of Compliance. This form can be located at www.mtsu.edu/irb on the forms page.

Also, all research materials must be retained by the PI or **faculty advisor (if the PI is a student)** for at least three (3) years after study completion. Should you have any questions or need additional information, please do not hesitate to contact me.

Sincerely,

Andrew W. Jones
Compliance Office
615-494-8918
Compliance@mtsu.edu