EMPLOYEES' FAIRNESS PERCEPTIONS OF WORKPLACE SOCIAL MEDIA MONITORING: PRIVACY INVASIVENESS, SMARTPHONE OWNERSHIP, AND EMPLOYEE WORK PERIOD

by

Melissa N. McCord

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

Middle Tennessee State University
August 2018

Thesis Committee:

Dr. Judith Van Hein, Chair

Dr. Patrick McCarthy

Dr. Michael Hein

ABSTRACT

Electronically monitoring employee behavior is a controversial practice that expanded with Internet and email access on work computers and now includes social media activity on smartphones. Employers insist that monitoring not only protects their business interests but also creates a safe working environment; however, employees argue that monitoring could easily violate their privacy and is detrimental to organizational fairness. This study measured perceptions of fairness of current employees when presented with different scenarios depicting workplace social media monitoring. Relationships between privacy invasiveness, smartphone ownership, and employee work period (accessing social media activity while on- or off-duty) and their effects on perceptions of fairness for monitoring social media activity were examined. Main findings include a negative relationship between perceptions of fairness and privacy invasiveness where fairness perceptions decreased as the level of surveillance became more invasive. Findings also support a negative relationship between perceptions of fairness and smartphone ownership, where monitoring practices were perceived to be fairer for employees who accessed social media using work-issued smartphones instead their personal devices. Lastly, a significant two-way interaction between privacy invasiveness and employee work period indicated that perceptions of fairness and levels of privacy invasiveness differ depending on whether employees access social media while on- or off-duty. Responses supported a low level of monitoring for off-duty employees but increased to a medium level for on-duty employees. In all cases, the highest level of privacy invasiveness, which was using monitoring software to detect and report social media activity, was perceived most negatively.

TABLE OF CONTENTS

Page

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

CHAPTER I: INTRODUCTION

Social media plays a role in most employees' work lives (Olmstead, Lampe, & Ellison, 2015). According to a 2015 report by Pew Research Center about Social Media and the Workplace, employees use social media for work-related purposes like making or supporting professional connections (24%), getting information to help solve work issues (20%), and building or strengthening relationships with coworkers (17%) (Olmstead, Lampe, & Ellison, 2015). Using social media in a professional capacity can enhance worker productivity; however, it can also easily distract employees. In fact, employees admit the top two reasons they use social media at work is for personal reasons, like taking a mental break (34%) or communicating with friends and family (27%) (Olmstead, Lampe, & Ellison, 2015). In addition to productivity loss from recreational social media activity, other critical issues for management include employees (un)intentionally leaking proprietary information, harassing coworkers online, and potentially harming company reputation (Riedy & Wen, 2010). Employers largely combat these issues by electronically surveilling employees' Internet access and use including social media activity.

Whether a company has the legal and ethical right to review employees' emails or social media activity is up for debate. Employers assert monitoring protects their legitimate business interests and creates a safe working environment ("Managing Workplace Monitoring," 2016). Employees, however, argue monitoring violates their privacy, affects fairness judgments, their quality of life, and trust, and due process (Tabak & Smith, 2005).

Electronic surveillance is defined as the "use of computerized systems to automatically collect, store, analyze, and report information about employee behavior"

(Riedy & Wen, 2010). It differs from traditional forms of surveillance by monitoring many employees simultaneously, gathering highly detailed information, and possibly creating an atmosphere that the "boss is always watching" (Riedy & Wen, 2010). Legally, electronic employee surveillance resides in a gray area, which is further complicated by nonexistent federal statutes and a sometimes contradictory mishmash of state and local laws (Firoz, Taghi, & Souckova, 2005; Zimmerman, 2002). This study aims to better understand how (1) varying degrees of privacy invasiveness, (2) smartphone ownership (accessing social network sites with a personal smartphone versus a work-issued smartphone), and (3) accessing social network sites during different work periods (off-duty, authorized break versus on-duty, unauthorized break) will affect employees' perceptions of fairness when their employers monitor personal social media activity. Arguments for and against monitoring employees and relevant consequences are discussed.

Social Network Sites (SNS)

Boyd and Ellison (2008) define social network sites (SNS) as "web-based platforms that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system" (Boyd & Ellison, 2008, p. 211). SNSs like Facebook, LinkedIn, YouTube, and Twitter were designed to share information and interact with other users (Smith & Kidder, 2010). The emergence and growth of SNS over the last decade is staggering. When Pew Research Center first began to track social media use in 2005, only 5% of the American population used at least one SNS ("Social Media Fact Sheet," 2017). By 2011,

the number rose to 50%, and today, 69% of the public uses some type of SNS to connect, share information and news, and entertain themselves ("Social Media Fact Sheet," 2017). With the wider adoption of social media, its user base has become more representative of the larger population. The most-widely used SNS, Facebook, fits this profile. Sixty-eight percent of U.S. adults use Facebook as of April 2016 ("Social Media Fact Sheet," 2017). Other popular SNSs include Instagram (owned by Facebook) (used by 28% of U.S. adults), Pinterest (26%), LinkedIn (25%), and Twitter (21%). Unlike these SNS, however, Facebook has not experienced significant growth since between 2012 and 2015 (Duggan, 2015). Nevertheless, Facebook still has the most engaged users with 76% reporting daily visits (Waring & Buchanan 2010; "Social Media Fact Sheet," 2017).

When Facebook users accept a friend request, both parties can view each other's profiles, which contain a wealth of personal information like what the user is doing, who the user is interacting with, and where the user is at any moment (Smith & Kidder, 2010; Stoughton, Thompson, & Meade, 2013; Karlen, 2014). Even organizations can join Facebook among other SNSs and interact directly with their customers. This allows organizations to conduct market research, offer tailored promotions, and contact users for recruiting purposes. However, organizations, can also have sinister intentions and push unwanted advertising on users or spy on customers' actions and behaviors (Karlen, 2014).

Electronic Monitoring of Current Employees

Organizations have always monitored employees (Alder, Ambrose, & Noel, 2006). The transition from analogue to digital surveillance methods was a particular turning point since a large amount of information could now be stored, transmitted, and

retrieved cheaply and clandestinely ("Workplace Privacy and Employee Monitoring," 2017; McDonald & Thompson, 2016). As a result, nearly every action an employee performs at work can be monitored and measured including SNS access and Internet use (Katz, 2016).

Common forms of monitoring include tracking computer content, keystrokes, and time spent using a keyboard. According to 2007 electronic monitoring and surveillance survey by the American Management Association (AMA) and The ePolicy Institute, 43% of employers store and review computer files, 12% monitor "the blogosphere" to keep tabs on company reputation, and 10% regularly monitor SNSs ("Electronic Monitoring," 2007). Disturbingly, Deloitte LLP's 2009 Ethics & Workplace Survey found that 30% of business executives admitted to informally monitoring SNS ("Social Networking," 2009). No other reports of informal monitoring could be found at this time. Other forms of surveillance include watching employees via CCTV, recording telephone calls, monitoring office computer screens, and locating employees in buildings or company cars using GPS, key fobs, or electronic entry cards (McDonald & Thompson, 2016; Solon, 2015). Technology that alerts employers when employees install unauthorized programs is also widely available ("Workplace Privacy," n.d.).

Who or what monitors content also varies. The same AMA and The ePolicy Institute survey reported 73% of organizations use automation tools to monitor employee emails, and 40% assign an individual to physically read and review them ("Electronic Monitoring," 2007). The individual is from IT (73%), HR (34%), legal (18%), compliance (17%), an outside third-party (4%), or other (17%) ("Electronic Monitoring," 2007).

Mobile device monitoring. Employers commonly provide employees with mobile devices like cell phones, smartphones, and laptops for work purposes ("Workplace Privacy," n.d.). Under most circumstances, employers can legally monitor employees' company-owned mobile phones or devices ("Workplace Privacy and Employee Monitoring," 2017). Employers can also upload monitoring apps that secretly record text messages, emails, Internet access, location, contacts, call logs, photos, and videos. Employees are protected from electronic monitoring under certain circumstances like union contracts that can limit an employer's monitoring practices ("Workplace Privacy and Employee Monitoring," 2017). Public sector employees also have minimal protections under the U.S. Constitution's Fourth Amendment prohibiting unreasonable search and seizure. However, this safeguard is complicated when employees use company-owned equipment to send personal messages like in the U.S. Supreme Court case of City of Ontario v. Quon (2010) ("Workplace Privacy and Employee Monitoring," 2017). This case was the first to test privacy rights in the digital age and examined whether a city's police department violated an officer's rights by obtaining transcripts of sexually explicit text messages he sent using a wireless two-way text-messaging pager issued by his department (Totenberg, 2010). At the time, legal experts believed this case could have broad implications for how public and private employees may be monitored and also set legal precedence that applies to email, SNS, and using the Internet for personal purposes (Chen, 2010; Totenberg, 2010).

In 2002, the police department in Ontario, CA obtained transcripts and reviewed messages sent by the highest-volume user, Sergeant Jeff Quon, without his permission, to determine whether the monthly character limit for officers should be adjusted (Chen,

2010). Quon and the individuals he exchanged messages with sued the department. The 9th U.S. Circuit Court of Appeals ruled that Quon was protected from illegal searches and seizures under the Fourth Amendment and had a "reasonable expectation" of privacy when using his pager because he had been informed by a supervising lieutenant that officers could use their pagers for personal private use (Chen, 2010; Totenberg, 2010). Furthermore, Quon's representatives argued that the Ontario Police Department's "Computer Usage, Internet and E-mail Policy" did not explicitly cover pagers (Chen, 2010) The police department appealed to the U.S. Supreme Court, which unanimously ruled that the warrantless search was not an unreasonable violation of Quon's Fourth Amendment rights since the departmental audit was work-related.

However, the Quon decision was a more limited precedent than some experts had predicted. According to the majority opinion, the Court decided the case on the reasonableness of the pager audit and not whether Quon's asserted expectations of privacy were reasonable (Charles Rehberg v. James Paulk et al., 2010). Nevertheless, City of Ontario v. Quon (2010) was an early indicator of present-day arguments about mobile devices' increasing role in expanding employee surveillance beyond the workplace and whether employees have a right to privacy when using an employer-owned mobile device for personal reasons. This study will investigate employees' perceptions of fairness when they access social media using a personally owned smartphone compared to one that is provided by an employer. Based on lessons learned (or rather, not learned) from City of Ontario v. Quon, it is hypothesized that employees who use their personal smartphone to access SNS will find employer monitoring to be unjust.

Employer's Legitimate Business Concerns

Productivity. Companies track employees' "digital footprints" like SNS activity to identify inappropriate content as well as to ensure company time is not being spent for personal purposes (Thomas, Rothschild, & Donegan, 2014). Employers argue that their electronic equipment should be used for business purposes only and consider personal use as abusing resources and squandering productivity (Thomas, Rothschild, & Donegan, 2014; McDonald & Thompson, 2016). Some employees, however, seem to disagree. According to a 2012 Kelly Global Workforce Index, 30% of employees feel that using personal SNS at work is acceptable ("When Worlds Collide," 2012). Also, 24% believe it is acceptable to share opinions about work on personal SNS.

Survey evidence about employees' perceptions of personal SNS use at work and its effects on productivity is mixed. Pew Research Center's Social Media and the Workplace report found that 56% of employees believe using SNS at work ultimately helps their job performance, 22% believe it mostly hurts their job performance, and 16% feel it does not have much impact (Olmstead, Lampe, & Ellison, 2015). Conversely, the Kelly Global Workforce Index reported that 43% of employees believe using SNS at work adversely impacts their productivity ("When Worlds Collide," 2012). Riedy and Wen (2010) believe part of the reason for mixed evidence is because existing research does not separate the effects of surveillance from job design, equipment design, machine pacing, and "other potentially stressful aspects of a computer-based office worker" (Riedy & Wen, 2010, p. 90). Roberts & Sambrook (2014) contend that research measuring the amount of time employees spend on SNS during the workday does not differentiate whether the behavior occurs during authorized periods like lunch breaks or

unauthorized periods. For example, reports like Pew Research Center's Social Media and the Workplace that state 27% of employees use SNS to connect with friends and family while at work does not clarify when these behaviors occur (Roberts & Sambrook, 2014; Olmstead, Lampe, & Ellison, 2015). This study makes the distinction between employees who access SNS during a short break (off-duty) and while working (on-duty). It is hypothesized that employees who access SNS during short off-duty breaks will find employer monitoring to be unjust.

Fraud. Before the use of SNS became ubiquitous, lawyers would occasionally advise clients to physically surveil employees suspected of abusing the Family and Medical Leave Act (FMLA) (Smith, 2015). According to a speaker at the National Employment Law Institute's 2015 Employment Law Conference, this method often backfires (Smith, 2015). She recounted a scenario of an employee-under-surveillance who noticed a distinguishable car repeatedly driving by her house. The employee immediately recognized the vehicle as belonging to the company's lawyer. SNS monitoring prevents the temptation to physically tail a targeted employee in favor of easily collecting online evidence for employees suspected of FMLA abuse. In the case of Lineberry v. Detroit Medical Center et al. (2013), coworkers spotted questionable Facebook posts, reported them to a supervisor, and prompted an official investigation.

While on FMLA leave for a back and leg injury, Carol Lineberry posted Facebook photos of her vacation in Mexico that showed her riding in a motorboat, standing and holding two infant grandchildren, and other questionable activities for someone with an injury (Carol Lineberry v. Detroit Medical Center et al., 2013). Going on the planned, prepaid vacation was not the problem since Lineberry had been granted approval from

the physician who examined her for FMLA leave. Lineberry's supervisor was aware of the photos, having received copies of them from angry coworkers. When Lineberry emailed the supervisor expressing disappointment for not receiving a get-well card, the supervisor replied "the staff were waiting until you came back from your vacation in Mexico to determine the next step. Since you were well enough to travel on a 4+ hour flight, wait in customs lines, bus transport, etc., we were assuming you would be well enough to come back to work" (Carol Lineberry v. Detroit Medical Center et al., 2013, p. 2). Lineberry falsely stated she had used a wheelchair. Upon her return to work, Lineberry confessed during in-person inquiries when confronted with the photos. She was terminated for dishonesty and filed a complaint alleging her FMLA rights had been violated. The U.S. District Court for the Eastern District of Michigan sided with the employer. They ruled they employer had a legal right to fire Lineberry for dishonesty regardless of her FMLA status (Smith, 2015).

Negligent retention and supervision. Employers can be held responsible for the behavior of employees known to be a danger to others (Mooty, 2013). Most claims of negligent supervision involve employers who knowingly permitted or ignored inappropriate employee behaviors like harassment, violent or threatening behavior, signs of drug or alcohol abuse, or possession of weapons on work premises (Lewis & Gardner, 2000). However, negligent claims can also include instances when managers fail to swiftly respond once they "knew or should have known" an employee was a danger to others. Even in cases where an employer arguably did not know an employee presented a risk, the employer can still be held responsible (Lewis & Gardner, 2000, p. 16). An exception to this rule is Howard v. The Hertz Corporation (2016), a federal case about the

limits to which an employer should be held responsible for an employee's SNS activity (Satenberg, Bauman, Brunswick, Hudson, King, & Levy, 2016).

In 2012, a Hertz manager posted the following comment to Facebook about a customer he had interacted with earlier that day, "I seen Maurice [Howard]'s bougie ass walking kahului beach road… n**** please!" (Satenberg et al., 2016). Coworkers added comments and one "liked" the conversation. One of the manager's Facebook friends showed the post to the customer, Howard, who complained and sued Hertz. After considering claims of negligent training, retention, and supervision, the case was dismissed on the grounds that even though the manager had posted derogatory comments in the past, his post about the plaintiff was not foreseeable (Satenberg et al., 2016). Also, the manager's supervisor was not Facebook friends with him and therefore would not have seen the comments. Furthermore, the employee handbook about discriminatory language did not mention social media. Even though Howard v. The Hertz Corporation (2016) was dismissed, a company's decision to monitor employees' SNS activity could prevent dangerous individuals from harming other employees, avoid potentially devastating lawsuits, and earn organizational benefits like increased productivity and decreased employee turnover and absenteeism (Whitfield, 2013; Lewis & Gardner, 2000).

Confidential information. Employers also monitor SNS activity to prevent confidential information from being (un)intentionally leaked or shared with the public or industry competitors (Friedman & Reed, 2007; Lee & Kleiner, 2003; Lucero, Allen, & Elzweig, 2013; Rosenberg, 1999). Confidential information includes trade secrets, intellectual property, and employee files (Lee & Kleiner, 2003; Friedman & Reed, 2007;

Rosenberg, 1999). Confidential information is protected by law if (1) it is not obtainable via a publicly available source and (2) reasonable efforts have been taken to ensure confidentiality (Birmingham & Neumann, 2011). Once information is shared on SNS, you cannot "put the genie back in the bottle" (Birmingham & Neumann, 2011).

A 2009 Electronic Business Communications Policies & Procedures survey by the AMA and The ePolicy Institute suggested that employers are mainly concerned about security breaches and fear employees will disclose confidential information about the organization or its customers/patients ("Electronic Business Communications," 2009). Survey results stated that 61% of employers have policies prohibiting employees from discussing company secrets, financial data, and rumors or gossip on either the organization's or their personal SNS ("Electronic Business Communications," 2009). Results also confirmed employer worries about disclosing confidential information by indicating risks are on the rise. For example, 14% of employees reported they had emailed confidential or proprietary company information to outsiders, 6% said they had sent customers' confidential financial data (credit card numbers, social security numbers, etc.), and 6% said they had sent patients' protected health information (health status, medical care, payment issues, etc.) (Petrecca 2010). Even if employees do not intend to broadcast confidential information, posted social media content can be shared easily regardless of an individual's personal privacy settings.

Corporate reputation. CEOs and the public are increasingly interested in an organization's reputation partly because of the connection reputation has with competitive advantage and organizational performance (Ettenson & Knowles, 2007; Fombrun & Shanley, 1990). Maintaining a good reputation can increase profitability,

attract new applicants, investors, and customers, lower organizational costs, and serve as an incentive to sustain consumer-friendly prices (Roberts & Dowling, 2002; Fombrun, 1996; Turban & Greening, 1997). According to one researcher, corporate reputation is a company's most valued asset and ought to be protected at all costs (Coombs, 2007). Corporate reputation takes time to build, but once established, it can be relatively stable (Walker, 2010). However, SNS can damage reputation with little to no effort. Users can post false content, spread rumors, or conspire calculated attacks against targeted organizations (Horn, Taros, Dirkes, Huer, Rose, Tietmeyer, & Constantinides, 2015). Damaged reputations can lead to serious consequences like a loss of market share, decrease in stock price, lowered sales, and either harm to or the loss of relationships with key stakeholders (Horn et al., 2015).

Interestingly, current and former employees pose a greater threat to organizations than anonymous SNS users (Horn et al., 2015). In July 2013, a Golden Corral chef recorded video of raw hamburgers stored next to dumpsters and uploaded it to YouTube (Miles & Mangold, 2014; Wilkie, 2013; Roberts, 2013). The video went viral. The chef told ABC News he tried to file a complaint with management and notify the county health department about the meat's improper storage but was ignored. When official channels of communication failed, the chef felt compelled to take matters into his own hands. Even though Golden Corral disavowed the chef's recollection of events, it suffered damage to its reputation, public image, and most likely its market share and profitability (Miles & Mangold, 2014, Bennett, 2013).

Evident in the Golden Corral example, employees who either believe their voices will be ignored or who fear retribution can experience decreased work satisfaction and

may turn to SNS as a last resort (Miles & Muuka, 2011; Miles & Mangold, 2014). Employee dissent is a particularly serious reputational hazard because it suggests wider organizational problems, especially when complaints contradict an organization's identity. Simply offering official channels of communication like suggestion boxes or employee surveys is not enough because employees who distrust their organization and leadership are not likely to fully use them (Miles & Mangold, 2014; Detert & Burris, 2007). Distrust also leads to feelings of psychological vulnerability, which convinces employees they cannot properly evaluate potential risks associated with airing grievances via official channels (Miles & Mangold, 2014; Rousseau, 1995). Ultimately, employees who fall into this category are more likely to voice their dissent through social media, especially if they believe their organization does not monitor their SNS activities (Miles & Mangold, 2014).

Risks of Monitoring Employees' SNS Activity

Risks of monitoring employees' SNS activity include a lack of federal guidance, inconsistent state laws governing employees' privacy rights, concerted activity, and using a mobile device for both personal and business communications. Employers can still face legal challenges even when they have justifiable business reasons to monitor employees' SNS activity. Social media legal standards are in the early stages of development and are currently decided on a case-by-case basis (Morgan & Davis, 2013). To date, there are no federal statutes that clearly define an organization's rights to monitor and access employee SNS activity (Begley, Barras, Smoyer, & Haverstick, 2014).

Account-access statutes. In 2012, Maryland became the first state to prohibit employers from requiring or requesting personal SNS usernames and passwords from

applicants and employees (Begley et al., 2014; "Maryland is First State to Restrict," 2012). Also, employees are legally protected from discipline, termination, and other penalties if they refuse to grant SNS access to their employer (Whitfield, 2013). Account-access is often the only commonality among states' privacy laws and social media statutes (Begley et al., 2014). As of July 2016, 25 states and Guam have enacted similar laws with some exceptions (Whitfield, 2013). Organizations that operate in multiple states are forced to either apply the most restrictive rules to all locations or enact different standards for each location (Begley et al., 2014). Organizations and employees would greatly benefit from clear legal direction, especially on a national scale.

Off-duty conduct statutes. Employers seem to be largely concerned about liability when it comes to employees' SNS activity both on and off-the-clock (Chory, Vela, & Avtgis, 2016). Employers initially wanted to know about illegal activities employees engaged in, like theft or drug use, during off-duty hours (Pagnattaro, 2004). Now they are interested in legal activities like smoking, personal relationships, and lifestyle activities (i.e. alcohol), especially when documented on SNS. Currently, thirty states and the District of Columbia have "lifestyle discrimination" laws that protect employee privacy during off-duty hours (Pagnattaro, 2004; Whitfield, 2013). Most lifestyle discrimination laws specify off-duty activities like tobacco use, marital status or sexual orientation, political activity or affiliation, and arrest record or certain minor criminal convictions (Whitfield, 2013). Employees largely contend that their employers do not have the right to know about their off-duty activities and any attempt to gather this kind of information is an invasion of privacy (Lucero, et al., 2013; Pearce & Kuhn, 2003). Friedman and Reed (2007) suggest that organizations that expand surveillance

outside of the workplace risk increasing employee perceptions of privacy invasiveness, which can result in negativity and anger.

National Labor Relations Board and concerted activity. The National Labor Relations Act (NLRA) of 1935 defines and protects the rights and roles of employers, employees, and labor unions ("National Labor Relations Act," n.d.). Under the NLRA, employees have the right to self-organize, bargain collectively, strike, and picket. Employee rights stipulated in the NLRA are enforced by the National Labor Relations Board (NLRB), which investigates and prosecutes unfair labor practices (Whitfield, 2013). Section 7 of the NLRA grants employees the right to exercise "concerted activities for the purpose of collective bargaining or other mutual aid or protection" (Whitfield, 2013). According to NLRB rulings, this includes social media activity. In short, concerted activity occurs when two or more employees act together to protest or complain about employment terms and conditions such as wages or unsafe working conditions ("The NLRB and Social Media," n.d.). Section 8 of the NLRA prohibits employers from acting against employees who exercise concerted activity. The expanded definition means SNS posts and tweets may be recognized as concerted activity ("The NLRB and Social Media," n.d.). At the moment, the NLRB attempts to evaluate whether posts and tweets are protected concerted activity in the same manner as offline cases, even if SNS activity occurred during non-work hours (Lucero, et al., 2013). In cases where employee SNS communications are deemed concerted activity, the NLRB tries to follow traditional policies and procedures (Lucero, et al., 2013).

Bring-your-own-devices. Presently, 77% of the U.S. population owns a smartphone, rarely turns them off, and almost always have them within arm's reach

("Mobile Fact Sheet," 2017; "Privacy in the Age of the Smartphone," 2016). The proliferation of smartphones can partly be attributed to companies providing mobile devices or allowing bring-your-own-device (BYOD) to work policies (Chen, 2010). BYOD is a growing workplace trend that either allows or requires employees to use their personal mobile devices for work purposes instead of or in addition to employer-provided ones (Morgan & Davis, 2013; Begley et al., 2014; "Workplace Privacy and Employee Monitoring," 2017). Concurrently, an increasing number of employees choose to use the same mobile device for personal and work purposes and will voluntarily install employer's management software on their mobile devices ("Workplace Privacy and Employee Monitoring," 2017). BYOD is the latest challenge in balancing employers' motivation to secure data with employees' desire for privacy (Chen, 2010). In the current digital age, employees are often expected to be in constant contact with their managers (Chen, 2010). Anecdotally referred to as an "electronic leash", mobile devices extend surveillance beyond the workplace and into employees' homes. For employees who are used to toggling between work and personal communications throughout the day, this type of expanded surveillance may occur unwittingly (Chen, 2010).

Employees' Perceptions of Fairness

Privacy and the workplace. There are no federal or state statutes that prohibit private employers from monitoring employees' emails or websites (Riedy & Wen, 2010). Legal barriers used to combat employer surveillance like the Electronic Communications Privacy Act (ECPA), Stored Communications Act (SCA), and common law solutions and torts for invasion of privacy "are too porous to prevent electronic surveillance" for reasons beyond the scope of this study (Riedy & Wen, 2010, p. 92). While most

employees understand that anything they do using company-owned equipment is likely under surveillance, they may not realize ownership also includes the employer's electronic network (Thomas, Rothschild, & Donegan, 2014).

Federal electronic communications laws.

Electronic Communications Privacy Act (ECPA). The Electronic Communications Privacy Act of 1986 (ECPA) prohibits intercepting data transmissions at the time it occurs (Mooty, 2013; "Privacy in Employment," 2013). Specifically, the acts of intercepting, accessing, or disclosing electronic communications without prior authorization are prohibited. The idea of simultaneously monitoring and intercepting communications comes from ECPA's origins, which struck down wiretapping private telephone conversations and monitoring them during transmission (Ariss, 2002). However, the ECPA allows employers to monitor employees' electronic communications if (1) monitoring occurs in the regular course of business and (2) the employer owns the communication system that is being monitored ("Privacy in Employment," 2013). Put into context, monitoring intra-company email is usually acceptable, especially when communication is sent using employer-provided networks.

Employees who use third-party email providers like Gmail to exchange messages may create a "reasonable expectation of privacy" that shields their conversations from employer surveillance ("Privacy in Employment," 2013). In the 2010 case of Stengart v. Loving Care Agency, the New Jersey Supreme Court ruled in favor of Stengart, the employee who sent private emails to her attorney using a company-owned laptop and her personal Yahoo! account that were later removed from the hard drive's cache folder and read by her employer. The New Jersey Supreme Court ruled that under the circumstances,

Stengart could reasonably expect emails with her lawyer using a personal, password-protected, Internet-based account would remain private despite the fact that she used a company-owned laptop and violated her employer's electronic communications policy not to expect privacy when using employer-owned computers ("Workplace Privacy," n.d.; Innamarato & Krulewicz, 2010). Also, the company's electronic communications policy was found to be too vague and failed to define what it covered, including the extent to which communications would be monitored (Innamarato & Krulewicz, 2010). The policy's wording created doubt about whether emails are private or company-owned property. ECPA protections can also apply to SNS activity, which is discussed in the next section.

Stored Communications Act (SCA). The Stored Communications Act (SCA) is part of the ECPA and "prohibits the knowing or intentional unauthorized access to a facility through which an electronic communication service is provided" (Mooty, 2013, p. 17). For example, organizations that intentionally access employees' password-protected accounts without permission violate the SCA (Brandenburg, 2010). However, electronic service providers, namely, employers, are exempt and may access communications post-transmission without a legitimate business reason (Friedman & Reed, 2007). Ehling v. Monmouth-Ocean Hospital Service Corp. (2013) examined whether ECPA protections apply to SNS content (Klemchuk & Desai, 2014). In 2009, Deborah Ehling, a nurse, posted an impassioned opinion about a white supremacist who killed a security guard to her Facebook wall, which expressed her belief paramedics should have let the shooter die (Wohlgemuth, 2012). A coworker and Facebook friend sent screenshots of her post to hospital management (Klemchuk & Desai, 2014). After being disciplined, Ehling filed

suit alleging management's violation of the SCA by improperly accessing her Facebook wall (Klemchuk & Desai, 2014). The hospital argued that SNS like Facebook postings should have no expectation of privacy but the U.S. District Court for the District of New Jersey disagreed (Wohlgemuth, 2012). The court ruled that Ehling's efforts to restrict her Facebook wall to be private from supervisors and management fell within the scope of the SCA (Klemchuk & Desai, 2014). The court, however, did not address whether "a rant expressing an opinion" regarding a news event could be considered an expression of one's "private affairs" and therefore subject to privacy law protections (Wohlgemuth, 2012, p. 1).

Attitudes and consequences of electronic monitoring. The most current research on employees' perceptions to employer surveillance of their online usage including SNS is a 2016 empirical survey by Chory, Vela, and Avtgis. The study examined employees' perceptions of computer-mediated workplace communication privacy (CMWC is essentially electronic text-based communication tools used in an organization, like email and SNS) and beliefs about organizational justice (specifically procedural justice), trust in upper management, and commitment to their organization (Snyder 2010; Chory, et al., 2016). Organizational justice is the perception of fairness regarding organizational outcomes and processes, and procedural justice is the perceived fairness of the processes used to make decisions (Chory, et al., 2016). Chory, Vela, and Avtgis (2016) found that employees who perceived less CMWC privacy tended to view their organization's policies as less fair, placed less trust in upper management, and expressed less commitment to their organizations. These findings are pertinent to our study that measures employees' perceptions of fairness when employers monitor their

personal SNS. We too expect the level of privacy invasiveness of finding employee SNS activity will affect perceptions of fairness. Additional information about the study will be discussed in the next section.

Covertly monitoring employees' Internet use and SNS activity has the potential to cause distrust in the work culture by conveying an implicit message to employees that their employer does not trust them (Snyder, 2010). Other consequences include disrespect of management and poor interoffice relationships between employees and their supervisors (Alder, Schminke, Noel, & Kuenzi, 2007; Amick & Smith, 1992). Research by Alder, Ambrose, and Noel (2006) examined the effects of different implementation characteristics – advance notice, justification, and organizational trust –on employees' reactions to Internet monitoring (Alder, et al., 2006). They did not find evidence that attributes of the implementation process affect perceived fairness, contrary to previous evidence (Alder, et al., 2006). Results indicated that trust significantly influenced employees' perceptions of fairness, but neither advance notice nor justification for implementing a monitoring system had an effect.

More than half of the employees surveyed in the Kelly Global Workforce Index do not believe their employer has the right to view their SNS activity, which also extends to prospective employers ("When Worlds Collide," 2012). Similarly, Deloitte LLP's Ethics & Workplace Survey found that 53% of employees believe their SNS pages are none of their employers' business compared to 60% of executives who believe they have a right to know how employees portray the organization online ("Social Networking," 2009). Employees under electronic surveillance can experience increased physical and psychological stress, lowered quality of life from stress-induced illness, lowered work-

life balance, and lowered productivity (Amick & Smith, 1992; Tabak & Smith, 2005; Alder et al., 2007).

Monitoring SNS activity can also create lowered perceptions of organizational justice and organizational attractiveness in addition to increased opinions of privacy invasiveness (Stoughton, Thompson, & Meade, 2013). In a 2015 study, job applicants were informed that potential employers had collected information from their SNS for selection purposes. Applicants reported feelings of privacy invasiveness, which led to lower perceptions of organizational justice and organizational attractiveness in addition to increased intentions to sue the company (Stoughton, Thompson, & Meade, 2013). These findings were consistent for applicants who were offered a job and those who were not and can reasonably be extended to current employees.

Current Study

The tension between employers' use of surveillance for legitimate business reasons and employees' interest in privacy is a longstanding workplace issue (Allen, Coopman, Hart, & Walker, 2007). Matters became exponentially complicated once employers began to use SNS like Facebook as a business tool to identify problem employees. The lack of federal statutes or state privacy laws not only fails to provide clear ethical and legal boundaries but could also create a false sense of urgency with the potential for kneejerk reactions. In order to proactively address legitimate business issues, employers could easily justify expansive surveillance efforts that monitor employees' SNS activity (Begley et al., 2014; Allen et al., 2007). In response, employees who believe the surveillance is excessive or unjust may engage in acts of resistance like posting harmful or confidential information to SNS as a way to publicly humiliate individual

managers or the company as a whole (Allen et al., 2007). Whether individuals feel positively or negatively about SNS's influence in the workplace, most acknowledge the potential for shifting boundaries when employers infiltrate personal space (Del Bosque, 2013). This study will investigate how (1) varying degrees of privacy invasiveness, (2) smartphone ownership, and (3) periods of work will affect employees' perceptions of fairness when their employer monitors personal SNS activity. New insights and practical suggestions will hopefully help organizations craft social media policies that are not too broad or restrictive, are respectful of employees' privacy rights, and do not pose a threat to organizational justice (Riedy & Wen, 2010).

Primary research focus. How invasively an employer violates employees' privacy to find information about them on social media and its influence on fairness perceptions is of particular interest. The decision of whether a boss who uncovers an employee's Facebook post about work due to monitoring is justified to terminate the employee will be evaluated.

Hypothesis 1. Privacy invasiveness will be negatively related to employee perceptions of fairness. In other words, as the level of surveillance becomes more invasive, perceptions of fairness will be lower.

Hypothesis 2. Smartphones owned by employees will be negatively related to employee perceptions of fairness. For example, if social media is accessed using a smartphone that the employee owns, then perceptions of monitoring fairness will be lower. If the smartphone is owned by the employer, then perceptions of fairness will be higher.

Hypothesis 3. Social media activity that occurs during authorized short breaks (off-duty) will be negatively related to employee perceptions of fairness. For example, if an employee accesses social media during an authorized short break, then perceptions of monitoring fairness to be lower. If it is accessed during an unauthorized break, then perceptions of fairness will be higher.

Additional Research Question. The study is interested in how the independent variables will interact with each other and the ensuring effect on perceptions of fairness.

Research Question 1. Will privacy invasiveness, smartphone ownership, and work period interact? Will there be a 2-way or a 3-way interaction?

CHAPTER II: METHOD

Participants

Eligibility and informed consent. Survey participants had to be at least 18 years old and currently work in the United States. Skip logic was built into the survey in order to verify eligibility requirements. For example, participants who entered a text response that was less than 18 when prompted for their age were automatically skipped to the end of the survey thanking them for participation. The same process was used for work in the US – Participants who reported no for this item were skipped to the end of the survey. Skip logic was also used for a newly implemented and highly comprehensive informed courtesy of Middle Tennessee State University's (MTSU) Institutional Review Board (IRB). Participants who declined the informed consent were skipped to the end of the survey. It should be noted that no survey item forced responses. Participants were free to skip any questions, save and return to the survey at a later time, and review previous responses. Of the 1,192 recorded survey responses, 1,100 participants met eligibility requirements and agreed to the informed consent.

Attention check and debriefing items. Participants were asked the following attention check: "For quality assurance purposes, please select Agree". Before submitting the survey, participants were also asked two debriefing items that were created by Jacqueline Masso (2017) for her thesis. The two items were: "Did you take this study seriously, or did you click through the responses?"; "Is there any reason why we should NOT use your data?" No participants were removed for incorrectly answering these items.

Survey completion time. Pilot testing indicated the survey takes a minimum of 10 minutes. However, this stipulation removed 880 participants, leaving a sample size of 220, which was not enough power to detect large effects in the data during analyses. G*Power calculations indicated the necessary sample size to achieve a power of .80 with two-tailed tests and an α level of .05 was 360. This calculation is based on the fact that each participant will randomly receive one of twelve scenarios and then be asked questions about perceptions of fairness based on the narrative. A sample size of 360 means 30 participants per cell. See Appendix A.

The purpose of survey completion time is to ensure participants carefully read and answer all questions. However, it is possible the pilot tests were insufficient. Individuals who completed them personally knew this study's author and were also asked for feedback in terms of survey flow, confusing questions, and how long it took to complete. It is therefore possible these individuals were primed to take a longer amount of time to complete the survey. In light of this information, completion time was adjusted to a minimum of 7.5 minutes with a final sample size of 389 usable responses.

Demographics. Toward the end of the survey, participants were asked to self-report demographic information. There was a fairly even split between women and men (women comprised 53.3% of the study and men comprised 46.7%). Notably larger but not surprising divisions were found among participant age and ethnicity. Approximately half of participants were between the ages of 30 – 49 years old, 27.7% were between 18 – 29 years, and 15.9% were between 50 – 64 years. The overwhelming majority (77.2%) of participants identified as White; not Hispanic. Participants who identified as Black or

African American were the second largest ethnic group at 8.4%. See Appendix B – F for a detailed breakdown of demographics.

3x2x2 factorial design. The study was a between-subjects 3x2x2 factorial design that measured participants' perceptions of procedural fairness based on a randomly assigned scenario. In each scenario, a popular global coffee chain employee posts the following message on Facebook: "our customers would flip if they knew we toss recyclables in the same dumpster as trash. World's most ethical company my ass! #TasteofBeansCo". The boss becomes aware of the post and terminates the employee.

Scenarios measured the effects of three levels of privacy invasiveness when the boss monitors employees' social media activity (boss does a public search; a coworker shows the boss the post; monitoring software alerts the boss), two levels of the employee's smartphone ownership (employee posts using a personal smartphone; employee posts using a work-issued smartphone), and two levels of the employee's work period (employee posts during an authorized off-duty break; employee posts while on-duty when a break is not authorized). See Table 1 and Table 2 for details. An open-ended question asked participants to write why they rated their levels of agreement according to their assigned scenario. These comments allowed participants to explain their evaluations in their own words and supplemented quantitative data with qualitative information.

Table 1

3x2 Factorial Design with Employee's Personal Smartphone

Privacy Invasiveness	Off-Duty (authorized break) Employee Work Period	On-Duty (unauthorized break)
Low	Boss finds post via public search	Boss finds post via public search
Medium	Coworker shows post to boss	Coworker shows post to boss
High	Monitoring software alerts boss	Monitoring software alerts boss

Table 2

3x2 Factorial Design with Employee's Work-Issued Smartphone

Privacy Invasiveness	Off-Duty (authorized break) Employee Work Period	On-Duty (unauthorized break)
Low	Boss finds post via public search	Boss finds post via public search
Medium	Coworker shows post to boss	Coworker shows post to boss
High	Monitoring software alerts boss	Monitoring software alerts boss

Procedure

The survey was administered through Amazon Mechanical Turk (MTurk), a popular crowdsourcing marketplace (Ipeirotis, 2010). Evidence suggests MTurk is a good source for participants, who MTurk refers to as Workers, because they seem to represent the general population of Internet-users despite the fact that they tend to skew younger, have lower incomes, and smaller families (Ipeirotis, 2010). Workers complete posted human intelligence tasks (HITs) in exchange for a small monetary payment. Qualified Workers who successfully complete the survey received $0.75 for their participation. A HIT was created that stated the study's purpose, listed eligibility requirements, and informed Workers that surveys submitted under 8 minutes would not be accepted for payment. The HIT also contained a link that opened the survey in Qualtrics. Workers were instructed to manually input their MTurk Worker ID early in the survey to verify participation and receive payment. Additionally, they also received a randomly assigned survey code at the end of the survey and were instructed to copy-and-paste the survey code into a box located on the HIT's webpage.

Workers, now referred to as survey participants, were presented with a brief welcome message followed by MTSU's IRB informed consent and eligibility questions (age and work location). See Appendix K for the IRB approval letter. The informed consent stated survey participants' rights, disclosure information (e.g. survey's purpose, completing the survey more than once is prohibited), contact information, and the monetary amount for successful completion. Participants who met the screening criteria and electronically agreed to participate received measures relating to the following variables. See Appendix G for all survey items:

- Scenario (one of twelve randomly assigned scenarios)
- Social Network Site Usage
- Social Network Site Intensity
- Employee Experience with Previous or Current Monitoring
- Participant and Organizational Demographics
- Debriefing Questions

Demographic questions were reserved for the end of the survey to reduce possible effects of priming. None of the survey items required responses so participants could skip questions and return to previous pages. They also had the option to save their responses and complete the survey later.

Measures

Dependent variable

Fairness perceptions. The dependent variable for fairness perceptions was measured by three items. It is understood that Kimberly Kluesner (2013) originally created the items for her thesis and then Kelsey Bishop (2015) adapted and used them in her thesis. Participants were asked to rate their level of agreement about a scenario on a 5-point Likert scale (1-strongly disagree, 5-strongly agree):

1. "The monitoring practice is fair to the employee"
2. "The employer's decision to monitor employees is justified"
3. "Terminating this employee based on the monitoring practice is justified"

Independent variables

Privacy invasiveness. Privacy invasiveness is defined as the amount of effort an employer or boss expends in order to find information about an employee that is not

available in personnel files. The following items measured levels of privacy invasiveness from least to move invasive:

- Low: The boss does a public search and finds the employee's Facebook post
- Medium: A coworker who is Facebook friend's with the employee sees the Facebook post and shows it to the boss
- High: Monitoring software discovers the Facebook post and notifies the boss

Smartphone ownership. Smartphone ownership is defined as personal property that belongs to the person or entity that purchased it. The owner is also in charge of the smartphone's data. The following items measured levels of smartphone ownership:

- Personal: The employee purchased the smartphone and owns the device
- Work-issued: The corporation the employee works for purchased the smartphone, owns the device, and gave it to the employee for business purposes

Employee work periods. Employee work period is defined as an employee's work schedule. In this case, employees are authorized to take short breaks and may take care of personal matters during this time like calling a friend or checking social media. The following items measured different work periods:

- Off-duty break: An authorized short break granted to employees throughout the work day where work-related tasks can be momentarily paused

- On-duty: Normal working hours where employees are not authorized to take breaks and violations will likely result in reprimand or disciplinary actions

Scenarios. The dependent and independent variables were combined to create twelve narrative scenarios measuring participants' perceptions of fairness. Participants received one randomly assigned scenario and were asked to rate their level of agreement with the three items previously described for the dependent variable.

Social network site usage. Participants were asked whether they had personal social network account(s) with the following popular platforms: Facebook, Twitter, LinkedIn, Instagram, Pinterest, Snapchat, Tumblr, WhatsApp, YouTube, and a blank space for other. Participants who had personal social network account(s) were then asked how often they check them, report which one they visited most frequently, and how much time they typically spent using them.

Social network site intensity. This scale was adapted from the Facebook Intensity scale. It measures how personally connected a survey participant is to the social network sites he or she uses and has a reported Cronbach's alpha of .83 (Ellison, Steinfeld, & Lampe, 2007). The complete scale has six items and was originally used in Kluesner's (2013) study. Bishop (2015) only used three for her study's purposes, which will also be used in this study. Items omitted from the original scale included two that asked participants about their daily social media use, which was redundant to other scaled items in the demographics section. The third item asked if the participant was proud to be on social media, which was clearly outdated. The three retained items will inquire about the

participant's personal connectedness to social media beyond the scope of social media usage and scored on a 5-point Likert scale (1=strongly disagree, 5=strongly agree).

Experience with monitoring. Participants were asked whether they had ever assisted with or conducted employee monitoring in their current or previous job. Those who reported that they had were then asked to choose the type(s) of employee monitoring they had assisted with or conducted (surveillance videos, email screening, social media site screening, blogs, and a blank space for other). They were also asked how often their current or previous job required them to monitor current employees (rarely, occasionally, or frequently). These items were originally used by Kimberly Kluesner (2013) for her thesis and were then adapted by Kelsey Bishop (2015) to use in her thesis.

Demographics

Participants were asked to self-report personal demographic information which included their age range, gender, and ethnicity. Participants were then asked questions about their organizational demographics which included their job level (unemployed, not seeking employment; unemployed, seeking employment; part-time, full-time, student) and which industry best described their organization (business/professional services, financial services, government, manufacturing, public administration, wholesale/retail, education, and a blank space for other). The list of industries was borrowed from the 2009 Electronic Business Communications Policies & Procedures survey by the AMA and The ePolicy Institute ("Electronic Business Communications," 2009). Lastly, participants were asked to rate their level of agreement on a 5-point Likert scale (1-strongly disagree, 5-strongly agree) about whether they are satisfied with their current (or previous) boss and whether they felt loyal to their current (or previous) organization.

CHAPTER III: RESULTS

Demographic Correlational Analysis

Spearman's correlations were conducted for demographic items. See Appendix H for a correlation matrix and detailed summary of the relationships between survey items.

Preliminary Analyses

Reliability analyses were conducted to determine whether the three dependent variable survey items that comprise the fairness perception construct should remain separate or combined into a scale. Cronbach's alpha ranged from .81 to .96 across all twelve scenarios. Eight out of twelve scenarios had reliability analyses that indicated the following two dependent variable items, "The monitoring practice is fair to the employee" and "The employer's decision to monitor employees is justified", were not correlated. In these cases, Cronbach's alpha was lower with the two items combined than if kept separately or if combined with the third item, "Terminating this employee based on the monitoring practice is justified". See Appendix I for detailed results. Based on this information, it was determined that the dependent variable items "The monitoring practice is fair to the employee" and "The employer's decision to monitor employees is justified" would remain separate and not be combined into a scale for procedural fairness. However, the dependent variable item "Terminating this employee based on the monitoring practice is justified" would remain a rating of decision fairness.

For clarification purposes, the following dependent variables were renamed:

1) Fairness of Employee Monitoring ("The monitoring practice is fair to the employee")

2) Fairness of Decision to Monitor Employees ("The employer's decision to monitor employees is justified")
3) Fairness of Decision to Terminate Employees ("Terminating this employee based on the monitoring practice is justified")

Primary Analyses

Three 3x2x2 analyses of variance (ANOVAs) were conducted for the independent variables privacy invasiveness, smartphone ownership, and employee work period and each dependent variable. Welch analyses were used because each scenario had unequal sample sizes or population variances for all groups. See Appendix A for the frequency and percentage of participants by scenario. Welch tests assume each participant contributed one score and was not influenced by others in the study.

Fairness of Employee Monitoring (see Table 3) had main effects for privacy invasiveness and smartphone ownership, and a two-way interaction between privacy invasiveness and employee work period. Fairness of Decision to Monitor Employees (see Table 4) had a main effect for privacy invasiveness. Fairness of Decision to Terminate Employees (see Table 5) had neither main effects nor interactions.

Fairness of employee monitoring

A 3x2x2 ANOVA found three significant main effects for privacy invasiveness, smartphone ownership, and a two-way interaction between privacy invasiveness and employee work period. See Table 3 for details.

Post hoc analyses. Additional analyses (pairwise comparisons) were performed for privacy invasiveness and smartphone ownership to determine which levels were significantly different.

A one-way ANOVA using Games-Howell pairwise comparisons tested privacy invasiveness and found that two of the three levels were significantly different from each other. This finding indicated that performing public searches (low level) (M = 3.43), p .018 and relying on coworkers to report on their Facebook friends' activities (medium level) (M = 3.43), p = .020 were perceived to be fairer employee monitoring practices than using monitoring software (high level) (M = 3.03).

A Welch t-test for independent samples tested smartphone ownership (p = .038) and found that the two levels (e.g., personal smartphone and work-issued smartphone) were significantly different from each other. This finding indicated that employees believe monitoring a work-issued smartphone (M = 3.43, SD = 1.20, n = 185) is a fairer practice than monitoring their personal smartphone (M = 3.18, SD = 1.18, n = 204).

A one-way ANOVA using Games-Howell pairwise comparisons tested the interaction between privacy invasiveness and employee work period and found significant differences between the levels of privacy invasiveness (e.g., low, medium, and high) based on employee work period (e.g., off-duty and on-duty), $F(2, 377) = 4.36$, p = .013, partial $\eta^2 = 0.023$. When employees were off-duty (authorized break), performing public searches (low level) (M = 3.65) was perceived to be a fairer monitoring practice compared to using monitoring software (high level) (M = 3.11), p = .040. However, when employees were on-duty (unauthorized break), a higher level of privacy invasiveness, specifically relying on coworkers to report on their Facebook friends' activities (medium level) (M = 3.67), was perceived to be a fairer monitoring practice than using monitoring software (high level) (M = 3.13), p = .023. See Figure 1 for a summary display of the

interaction of privacy invasiveness and work period on perceptions of fairness of employee monitoring.

Table 3

3x2x2 ANOVA for Fairness of Employee Monitoring

Source	Type II Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	36.783	11	3.344	2.438	.006	.066
Intercept	4155.959	1	4155.959	3030.395	.000	.889
Privacy Invasiveness	11.568	2	5.784	4.217	.015	.022
Smartphone Ownership	5.621	1	5.621	4.099	.044	.011
Employee Work Period	1.800	1	1.800	1.312	.253	.003
Privacy Invasiveness * Smartphone Ownership	.350	2	.175	.128	.880	.001
Privacy Invasiveness * Employee Work Period	11.970	2	5.985	4.364	.013	.023
Smartphone Ownership * Employee Work Period	3.032	1	3.032	2.211	.138	.006
Privacy Invasiveness * Smartphone Ownership * Employee Work Period	1.504	2	.752	.549	.578	.003
Error	517.027	377	1.371			
Total	4792.00	389				
Corrected Total	553.810	388				

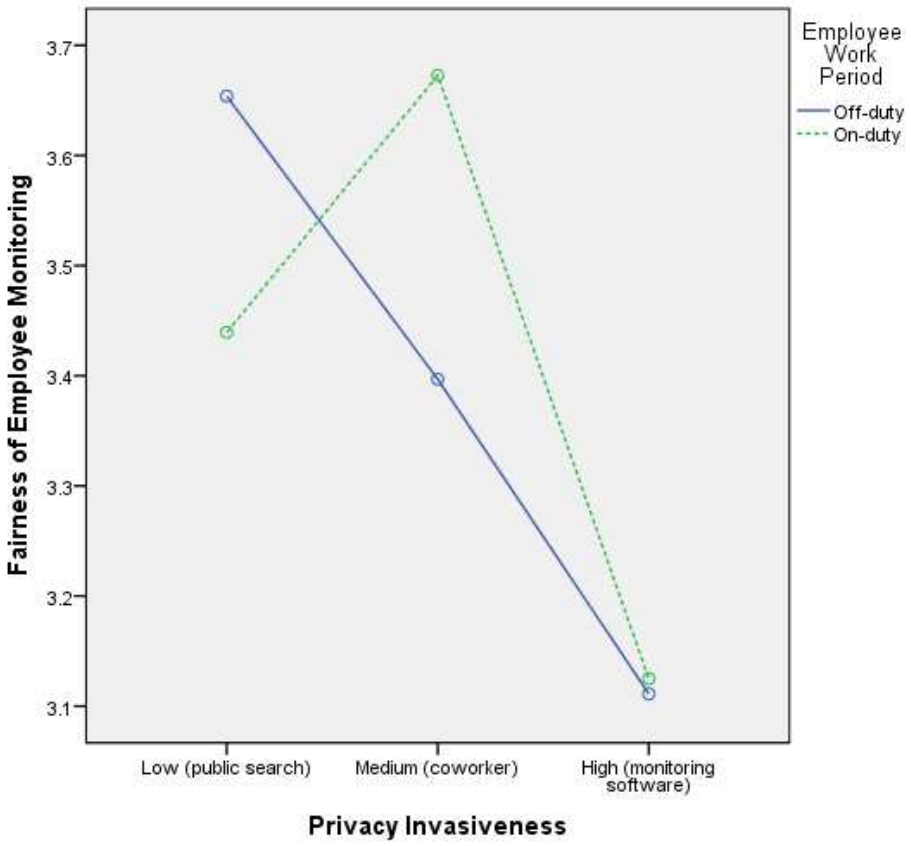

Figure 1. Fairness of Monitoring of Work Period and Privacy Invasiveness

Fairness of decision to monitor employees

A 3x2x2 ANOVA found a significant main effect for privacy invasiveness. See Table 4 for details.

Post hoc analyses. A one-way ANOVA using Games-Howell pairwise comparisons tested privacy invasiveness and found that two of the three levels were significantly different from each other. This finding indicated that the employer's decision to perform public searches (low level) (M = 3.56), p .011 and to rely on coworkers to report on Facebook friends' activities (medium level) (M = 3.53), p = .021

were perceived to be better justifications for monitoring employees than using monitoring software (high level) (M = 3.12)..

Table 4

3x2x2 ANOVA for Fairness of Decision to Monitor Employees

Source	Type II Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	29.379	11	2.671	1.843	.046	.051
Intercept	4423.443	1	4423.443	3052.852	.000	.890
Privacy Invasiveness	12.097	2	6.049	4.174	.016	.022
Smartphone Ownership	4.643	1	4.643	3.204	.074	.008
Employee Work Period	.020	1	.020	.014	.907	.000
Privacy Invasiveness * Smartphone Ownership	3.114	2	1.557	1.074	.343	.006
Privacy Invasiveness * Employee Work Period	3.912	2	1.956	1.350	.261	.007
Smartphone Ownership * Employee Work Period	1.551	1	1.551	1.071	.301	.003
Privacy Invasiveness * Smartphone Ownership * Employee Work Period	1.146	2	.573	.396	.674	.002
Error	546.256	377	1.449			
Total	5082.000	389				
Corrected Total	575.635	388				

Fairness of decision to terminate employees

A 3x2x2 ANOVA did not find main effects or significant interactions. However, it is worth noting that the interaction between privacy invasiveness and employee work period was nearly statistically significant, $p = .052$. See Table 5 for details.

Table 5

3x2x2 ANOVA for Fairness of Decision to Terminate Employees

Source	Type II Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	19.131	11	1.739	1.130	.336	.032
Intercept	4150.610	1	4150.610	2696.604	.000	.877
Privacy Invasiveness	5.066	2	2.533	1.646	.194	.009
Smartphone Ownership	.415	1	.415	.270	.604	.001
Employee Work Period	.165	1	.165	.107	.743	.000
Privacy Invasiveness * Smartphone Ownership	.127	2	.064	.041	.959	.000
Privacy Invasiveness * Employee Work Period	9.170	2	4.585	2.979	.052	.016
Smartphone Ownership * Employee Work Period	1.048	1	1.048	.681	.410	.002
Privacy Invasiveness * Smartphone Ownership * Employee Work Period	2.924	2	1.462	.950	.388	.005
Error	580.278	377	1.539			
Total	4831.000	389				
Corrected Total	599.409	388				

Additional Results

Social network usage

The tested items for Social Network Usage were "How often do you check social media?" and "How much time do you typically spend using the social media platform you visit most frequently?" An analysis of covariance (ANCOVA) procedure was planned to compare group means of the dependent variables when controlling for the two Social Network Usage items. However, ANCOVA is sensitive to assumption violation and the first of three preliminary tests (polynomial test, homogenous slopes test, and group differences on the covariate) that occurred prior to conducting an ANCOVA did not yield any significant relationships. Since higher order polynomial testing is outside the perimeter of this study, ANCOVA will not be used to examine Social Network Usage.

How often employees check social media. A familywise alpha of .05 was used for all analyses. The relationships between social network usage and the dependent variables were explored using polynomial regression. However, none of the linear nor quadratic relationships were significant (Fairness of Employee Monitoring for linear test, t (384) = -0.27, p = .791, and quadratic test, t (384) = -0.65, p = .515; Fairness of Decision to Monitor Employees for linear test, t (384) = -0.62, p = .537, and quadratic test, t (384) = -0.41, p = .681; Fairness of Decision to Terminate Employees for linear test for, t (384) = -0.002, p = .999, and quadratic test, t (384) = -0.17, p = .862).

Amount of time spent on social media platform visited most frequently. A familywise alpha of .05 was used for all analyses. The relationships between social network usage and the dependent variables were explored using polynomial regression. However, none of the linear nor quadratic relationships were significant (Fairness of

Employee Monitoring for linear test, t (385) = -0.93, p = .354, and quadratic test, t (385) = 0.77, p = .440; Fairness of Decision to Monitor Employees for linear test, t (385) = -1.69, p = .093, and quadratic test, t (385) = 0.99, p = .318; Fairness of Decision to Terminate Employees for linear test for, t (385) = -0.49, p = .620, and quadratic test, t (385) = -0.18, p = .860).

Qualitative comments

Each participant was asked "Why did you react that way? Please be as specific as possible" following the scenario. The open-ended item was included in the survey in order to add meaning to quantitative data. Responses allowed participants to write about their reactions to the scenario and explain reasons for selecting levels of agreement in their own words. Comments will be addressed in the Discussion section. See Appendix J.

CHAPTER IV: DISCUSSION

Previous research by Kluesner (2013) and Bishop (2015) found significant main effects that indicated employee perceptions of fairness decreased as the level of privacy invasiveness increased for both procedural and decision fairness. This study also found significant main effects for privacy invasiveness but differed in terms of reliability analyses. Kluesner's (2013) and Bishop's (2015) individual reliability analyses suggested combining two of the three dependent variable items ("The monitoring practice is fair to the employee" and "The employer's decision to monitor employees is justified") into a construct representing procedural fairness. The third tem ("Terminating this employee based on the monitoring practice is justified") remained separate and represented decision fairness. However, reliability analyses for this study did not support combining any of the three fairness items, which resulted in three separate constructs of fairness: (1) Fairness of employee monitoring ("Monitor Employees"), (2) fairness of the decision to monitor employees ("Decide to Monitor Employees"), and (3) fairness of the decision to terminate employees based on monitoring ("Terminate Employees").

Perhaps the conflict between employer monitoring and taking personal responsibility for public online comments, represented by fairness to (1) "Monitor Employees" and (2) "Decide to Monitor Employees", is a third, unknown fairness construct separate from process and decision fairness. Both items may still be categorized as procedural fairness but the first is fairness of employee monitoring theoretically and the second could be adapting theory to reality. More than half of the open-ended comments suggest an individualistic arguably American notion of individual rights including privacy. For example, fairness to (1) "Monitor Employees" seems to conjure

notions of individual freedom and an inherent distrust of being monitored. However, opinions change when the idea is applied to the workplace. Participants may think of privacy in terms of their own organization and personal experiences when asked about fairness to (2) “Decide to Monitor Employees”. In the words of one participant, “I feel like you should be held responsible for things you say but i also feel like work shouldn’t be looking through your personal social media. Also I feel that people need to be aware of what’s public online”. Another explanation for the conflict between fairness to (1) “Monitor Employees” and (2) “Decide to Monitor Employees” could be socially acceptable answers.

In general, participants believed that lower levels of monitoring were fairer than higher levels of monitoring. However, perceptions of fairness changed depending on whether an employee was on a break (off-duty) or working (on-duty), which supports a two-way interaction between fairness of monitoring of work period and privacy invasiveness for fairness to (1) “Monitor Employees” but not (2) “Decide to Monitor Employees” or (3) “Terminate Employees”. Perceptions of fairness decreased as privacy invasiveness increased for off-duty employees, which supports the first hypothesis for fairness to (1) “Monitor Employees” and (2) “Decision to Monitor Employees”.

Findings for off-duty employees coincide with research about off-duty conduct statutes. Lucero, Allen, and Elzweig (2013) explain that employees believe that their employers do not have a right to know about their off-duty activities, and attempts to gather information about them outside of work is an invasion of privacy (Pearce & Kuhn, 2003). Friedman and Reed (2007) warn that plans to expand surveillance beyond the

workplace risks increasing employees' perceptions of privacy invasiveness, which can lead to negativity and anger.

A predominant theme in the open-ended survey comments expands upon this trend. There appears to be a general distaste for monitoring (perhaps best expressed by the comment "Butt out, Big Brother!") with two stipulations. First, employees who get caught only have themselves to blame, which is best expressed by the comment "I feel like it is wrong for companies to monitor social media, but that being said, if you do something stupid on social media and your company finds out, it's kind of your own fault if you get in trouble or fired!" Second, employees who violate social media policies must face consequences, which addresses fairness to (2) "Decide to Monitor Employees". Whether the fictional company had a social media policy was a recurring inquiry with favorability generally on the side of the employer:

> I don't recall if there is a social media policy in effect that the employee signed and if she was aware of the monitoring. So I'm conflicted because if she knew she'd be fired then it's fair. However if there was no policy than I side with her. I don't think people in most positions should be fired for social media posts. I also don't like the monitoring but if it's in the company's policy...

More than half of the comments expressing distaste for workplace monitoring mentioned feelings of conflict, such as "Overall, I am rather conflicted on the topic of cybervetting. Part of me believes that employees should be fully responsible for what is posted and shared to their social media account. Another part of me is kinda turned off by the fact that you have your manager going out of his way to look up your profile. (not in this case, but speaking in general)"

Compared to off-duty employees, the picture for on-duty employees and the relationship between fairness of monitoring of work period and privacy invasiveness is more nuanced. As privacy invasiveness increased, perceptions of fairness initially increased but then decreased. In other words, participants thought that increasingly invasive monitoring practices were fair for on-duty employees up to a point, which is a medium level. The result is an increase in perceptions of fairness as privacy invasiveness increased from a low to a medium level followed by a change in opinion as privacy invasiveness increased from a medium to a high level.

Findings for on-duty employees at higher levels of privacy invasiveness support the first hypothesis and echo results from the Kelly Global Workforce Index, which found that more than half of surveyed employees do not believe their employer has the right to view their SNS activity ("When Worlds Collide," 2012). Another source of support is Deloitte LLP's Ethics & Workplace Survey, which found that 53% of employees believe their SNS pages are none of their employers' business ("Social Networking," 2009).

Findings for on-duty employees at lower levels of privacy invasiveness do not support the first hypothesis and seem to largely go against the small amount of workplace SNS literature that currently exists. It is difficult to discuss this trend because workplace SNS research broadly does not distinguish work period. For example, neither the Kelly Global Workforce Index nor Deloitte LLP's Ethics & Workplace Survey differentiate whether employee behavior (and beliefs about behavior) occurs during authorized off-duty periods like lunch breaks or unauthorized on-duty periods (Roberts & Sambrook, 2014). Discussion about perceptions of fairness at lower levels of privacy invasiveness and why it changes direction is therefore limited. At best, we can surmise that a medium

level of privacy invasiveness seems to be a sweet spot that employers can exploit before employees feel their privacy has been violated while on-duty.

No main effects support the third hypothesis, which stated that monitoring will be perceived as fairer when employees access social media off-the-clock (off-duty) rather than while working (on-duty). Support was only found for the interaction between fairness of monitoring of work period and privacy invasiveness as previously discussed.

Smartphone ownership also had a significant impact on perceptions of fairness. Employees perceived monitoring work-issued smartphones to be fairer than monitoring employees' personal smartphones, which supports the second hypothesis for fairness to (1) "Monitor Employees" but not for (2) "Decide to Monitor Employees" or (3) "Terminate Employees". Open-ended comments were very clear that work-issued property should only be used in a professional capacity. For example, one comment stated "The fact of the matter is that she used the company phone. What world is it ok to talk bad about your employer via their own equipment? If she had rather done this on her own accord using her own devices it would be a little more acceptable" Another theme was concern for corporate reputation and brand/image. Similar to the Golden Corral chef who recorded video of raw hamburgers next to dumpsters and uploaded it to YouTube in July 2013 after his complaints were ignored, survey participants voiced concern about employees posting damaging information since "Corie is the image of the company and should have been professional" (Miles & Mangold, 2014; Wilkie, 2013; Roberts, 2013; Horn et al., 2015). As in the Golden Corral example, some commenters upheld employees' rights to be heard even if it risks reputation:

> I'm in the middle on this one. I believe that you should always keep your work life off of a social media. On the other hand, if you are aware of the circumstances and feel you should be "heard" about certain situations, then post away. I don't think the employee should've been fired, more as, given a warning instead and fix the problem the employee was stating.

Furthermore, a handful of commenters understood that current and former employees pose a greater threat to corporate reputation than anonymous SNS represented by the statement “One employee can destroy a business, even if the accusation is true.” Evident in the previous section, this same commenter also inquired about the company’s social media policy/guideline/contract by stating “The business however, should have it clearly outlined in the work contract that this behavior is not allowed. There should be a way to inform the bosses without going to social media.”

Privacy invasiveness had a notable influence on perceptions of fairness to (1) “Monitor Employees” and (2) “Decide to Monitor Employees” but not to (3) “Terminate Employees”. A possible reason fairness to (3) “Terminate Employees” lacked main effects is a widespread distaste for terminating employees because of SNS activity. For example, one participant wrote “I really don't think the employee should've been fired. May tell them if they ever did anything like that again they would be but not fire them “. It is possible that checking social media throughout the day has become so common and easy via smartphones that it is widely viewed to be inoffensive. This argument is supported by survey demographic information where 65.6% of respondents reported visiting social network sites daily and 36.8% claimed to spend between 10 to 30 minutes at a time (see Appendix D for complete social network site demographics). Furthermore,

approximately 22% reported spending between 31 and 60 minutes and another 22% reported spending less than 10 minutes, which suggests frequent daily social media activity for brief amounts of time.

Limitations and Future Research

This was an exploratory study about an emerging topic that currently lacks peer-reviewed research about employee attitudes and opinions about workplace social media monitoring. An obvious limitation is the lack of replicated studies, which complicates generalizing results. Other limitations include possible historical bias. Survey participants were not asked about their social media history (i.e., how long they have used certain platforms) or their personal opinions about social media privacy, which would influence how they rate the narrative scenarios. Another limitation was survey completion time. The amount of time it took participants to complete the survey was noticeably different between pilot tests (minimum of 10 minutes) and the live survey. Applying a 10 minimum cutoff to 1,100 participant responses reduced the sample size by 80%. Completion time was reduced to 7.5 minutes in order to maintain .80 power with an α level of .05. The final sample size of 389 based on a calculated minimum of 360 was sufficient but not ideal.

There is ample room for future research. Social networks are largely unregulated and change rapidly based on user preferences and platform popularity. For example, Kluesner (2013) included MySpace in her survey because it was still a relatively common and widely used service. Its relevance is miniscule today and therefore MySpace was not included in this survey nor mentioned by participants. Future research should consider other legitimate business concerns and how they relate to employee perceptions of

workplace social media monitoring fairness. Suggestions include workplace surveillance finding protected Americans with Disabilities Act of 1990, Genetic Information Nondiscrimination Act of 2008, and Title VII of the Civil Rights Act of 1964 information. Discovering online evidence of employees' risqué pictures, recorded illegal activity, or evidence of FMLA fraud are other ideas. Also, workplace safety issues, negligent retention of hostile employees, and attacks against an organization's reputation and/or brand would also be interesting topics.

A research area for those interested in emerging technology is examining wearable/smart devices like fitness trackers and GPS-enabled devices that employers will sometimes bestow to employees as gifts. Lastly, volunteer-based programs that implant Radio Frequency ID (RFID) chips in employees' hands are an affordable and growing trend. With a wave of the hand, implanted microchips can open doors, pay for purchases, store medical information, share business cards, and even login to computers. This study's author sincerely hopes that research can catch up; after all, Facebook will not remain the worldwide social network of choice forever. It is possible, even arguably likely, that Facebook will cease to be commonplace within the next five years like MySpace in favor of workplace wearables.

REFERENCES

Allen, M.W., Coopman, S.J., Hart, J.L., & Walker, K.L. (2007). Workplace surveillance and managing privacy boundaries. *Management Communication Quarterly*, *21*(2), 172-200.

Alder, G.S., Ambrose, M.L. & Noel, T.W. (2006). The effect of formal advance notice justification on Internet monitoring fairness: Much ado about nothing? *Journal of Leadership and Organizational Studies*, *13*(1), 93-108.

Alder, G.S., Schminke, M., Noel, T.W., & Kuenzi, M. (2007). Employee reactions to Internet monitoring: The moderating role of ethical orientation. *Journal of Business Ethics*, *80*(3), 481-498. doi:10.1007/s10551-007-9432-2

Amick, B.C. III, & Smith, M.J. (1992). Stress, computer-based work monitoring and measurement systems: A conceptual overview. *Applied Ergonomics*, *23*(1), 6-16.

Ariss, S.S. (2002). Computer monitoring: Benefits and pitfalls facing management. *Information & Management*, *39*(7), 553-558. doi:10.1016/S0378-7206(01)00121-5

Begley, S.A., Barras, J.S., Smoyer, D., & Haverstick, A.D. (2014) *Perils and pitfalls: Social media law and the workplace*. Retrieved from http://www.instituteforlegalreform.com/uploads/sites/1/ILR_SocialMedia_R6.pdf

Bennett, R. (2013, October 6). *Golden Corral disputes social media charges of uncleanliness*. Retrieved from http://www.kpho.com/story/22783430/golden-corral-disputes-social-media-charges-of-uncleanliness

Birmingham, J.F., & Neumann, J.L. (2011, March 25). Social media and the workplace: Beware of disclosure of trade secret and confidential information. *Michigan Lawyers Weekly*. Retrieved from http://go.galegroup.com.ezproxy.mtsu.edu/ps/i.do?p=AONE&u=tel_middleten&id=GALE%7CA252901286&v=2.1&it=r&sid=ebsco&authCount=1

Bishop, K. (2015). *What's your status: Employee fairness perceptions of social media monitoring*. Retrieved from JEWLScholar@MTSU Repository.

Boyd, D.M., & Ellison, N.B. (2008). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication, 13*(1)*,* 210-230.

Brandenburg, C. (2010). The newest way to screen job applicants: A social networker's nightmare. *Federal Communications Law Journal, 60*(3)*,* 597-626.

Carol Lineberry v. Detroit Medical Center et al., No. 11-13752 (United States District Court Eastern District of Michigan Southern Division, February 5, 2013).

Charles Rehberg v. James Paulk et al., No. 09-11897 (United States Court of Appeals, Eleventh Circuit, July 16, 2010).

Chen, S. (2010, April 20). Personal texting on a work phone? Beware your boss. *Cable Network News*. Retrieved from http://www.cnn.com/2010/LIVING/worklife/04/20/work.text.email.privacy/index.html

Chory, R.M., Vela, L.E., & Avtgis, T.A. (2016). Organizational surveillance of computer-mediated workplace communication: Employee privacy concerns and responses. *Employee Responsibilities & Rights Journal, 28*(1), 23-43. doi:10.1007/s10672-015-9267-4

Coombs, W. T. (2007). Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. *Corporate Reputation Review*, *10*(3), 163-176.

Del Bosque, D. (2013). Will you be my friend? Social networking in the workplace. *New Library World*, *114*(9/10), 428-442.

Detert, J.R., & Burris, E.R. (2007). Leadership behavior and employee voice: Is the door really open? *Academy of Management Journal*, *50*(4), 869-884.

Duggan, M. (2015, August 19). Mobile messaging and social media 2015. *Pew Research Center: Internet & Technology*. Retrieved from http://www.pewinternet.org/2015/08/19/mobile-messaging-and-social-media-2015/

Deborah Ehling v. Monmouth-Ocean Hospital Service Corp., No. 2:11-cv-03305 (WJM) (United States District Court for the District of New Jersey, August 20, 2013).

Electronic business communications policies & procedures survey (2009). *The ePolicy Institute*. Retrieved from http://www.epolicyinstitute.com/2009-electronic-business-communication-policies-procedures-survey-results

Electronic monitoring & surveillance survey (2007). *The ePolicy Institute*. Retrieved from http://www.epolicyinstitute.com/2007-survey-results

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*(4), 1143-1168-498. doi:10.1111/j.1083-6101.2007.00367.x

Ettenson, R., & Knowles, J. (2007). Don't confuse reputation with brand. *MIT Sloan Management Review*, *49*(2), 19-21.

Firoz, N.M., Taghi, R., & Souckova, J. (2005). E-mails in the workplace: The electronic equivalent of "DNA" evidence. *Journal of American Academy of Business*, *8*, 71-78.

Fombrun, C.J. (1996). *Reputation: Realizing value from the corporate image*. Boston, MA: Harvard Business School Press Books.

Fombrun, C., & Shanley, M. (1990). What's in a name? Reputation building and corporate strategy. *Academy of Management Journal, 33*, 233–258. doi:10.2307/256324

Friedman, B.A., & Reed, L.J. (2007). Workplace privacy: Employee relations and legal implications of monitoring employee e-mail use. *Employee Responsibilities & Rights Journal*, *19*(2), 75–83. doi:10.1007/s10672-007-9035-1

Held, A. (2018, April 4). Facebook says Cambridge Analytica data grab may be much bigger than first reported. *National Public Radio*. Retrieved from https://www.npr.org/sections/thetwo-way/2018/04/04/599542151/facebook-says-cambridge-analytica-data-grab-may-be-much-bigger-than-first-report

Horn, I.S., Taros, T., Dirkes, S., Huer, L., Rose, M., Tietmeyer, R., & Constantinides, E. (2015). Business reputation and social media: A primer on threats and responses. *Journal of Direct, Data and Digital Marketing Practice*, *16*(3), 193-208.

Innamarato, D.A. & Krulewicz, E.D. (2010, April 29). New Jersey high court limits employer's right to review employee emails. *Reed Smith LLP*. Retrieved from https://www.employmentlawwatch.com/2010/04/articles/employment-us/new-jersey-high-court-limits-employers-right-to-review-employee-emails/

Ipeirotis, P.G. (2010). Analyzing the Amazon Mechanical Turk marketplace. *XRDS: The ACM Magazine for Students, 17*(2), 16-21. doi:10.1145/1869086.1869094

Karlen, J.M. (2014). Privacy: Expectations and employment. *Business Management Dynamics, 3*(10), 28-36.

Katz, L.M. (2016, June 1). *Monitoring employee productivity: Proceed with caution*. Retrieved from https://www.shrm.org/hr-today/news/hr-magazine/pages/0615-employee-monitoring.aspx

Klemchuk, D.M., & Desai, S. (2014). Can employer monitoring of employee social media violate the Electronic Communications Privacy Act? *Intellectual Property & Technology Law Journal*, *26*(2), 9-13.

Kluesner, K.E. (2013). *Fairness perceptions of screening social networking sites for hiring decisions*. Retrieved from JEWLScholar@MTSU Repository.

Lee, S., & Kleiner, B.H. (2003). Electronic surveillance in the workplace. *Management Research News, 26*(2-4), 72-81.

Lewis, K. & Gardner, S. (2000). Looking for Dr. Jekyll but hiring Mr. Hyde: Preventing negligent hiring, supervision, retention, and training. *Journal of Healthcare Protection Management: Publication of the International Association for Hospital Security*, *78*(1), 14-22.

Lucero, M.A., Allen, R.E. & Elzweig, B. (2013). Managing employee social networking: Evolving views from the National Labor Relations Board. *Employee Responsibilities & Rights Journal*, *25*(3), 481-498. doi:10.1007/s10672-012-9211-9

Managing workplace monitoring and surveillance (2016, February 18). *Society for Human Resource Management*. Retrieved from https://www.shrm.org/resourcesandtools/tools-and-samples/toolkits/pages/workplaceprivacy.aspx

Maryland is first state to restrict employer demands for employee, applicant passwords. (2012, June). *HR Focus, 89*(6), 15, ISSN:10596038

Masso, J. (2017). *Supervisor, coworker, and organizational supportiveness of flexible work-life balance policies and its impact on perceived promotion probability*. Retrieved from JEWLScholar@MTSU Repository.

Maurice Howard v. The Hertz Corporation et al., No. 13-00645 (United States District Court for the District of Hawaii, January 25, 2016).

McDonald, P. & Thompson, P. (2016). Social media(tion) and the reshaping of public/private boundaries in employment relations. *International Journal of Management Reviews*, *18*(1), 69-84, doi:10.1111/ijmr.12061

Miles, S.J., & Mangold, G.W. (2014) Employee voice: Untapped resource of social media time bomb? *Business Horizons*, *57*(3), 401-411.

Miles, S.J., & Muuka, G.N. (2011) Employee choice of voice: A new workplace dynamic. *Journal of Applied Business Research*, *27*(4), 91-103.

Mobile fact sheet. (2017, January 12). *Pew Research Center: Internet & Technology*. Retrieved from http://www.pewinternet.org/fact-sheet/mobile/

Mooty, G.P. (2013, July). The legal guide to the use of social media in the workplace. *Minnesota Department of Employment and Economic Development*. Retrieved from https://mn.gov/deed/assets/legal-guide-social-media-workplace_tcm1045-133709.pdf

Morgan, H.A. & Davis, F.A. (2013, March) Social media and employment law summary of key cases and legal issues. *Paul Hastings LLP*. Retrieved from https://www.americanbar.org/content/dam/aba/events/labor_law/2013/04/aba_national_symposiumontechnologyinlaboremploymentlaw/10_socialmedia.authcheckdam.pdf

National Labor Relations Act. (n.d.). *National Labor Relations Board*. Retrieved from https://www.nlrb.gov/resources/national-labor-relations-act

The NLRB and social media (n.d.). *National Labor Relations Board*. Retrieved from https://www.nlrb.gov/news-outreach/fact-sheets/nlrb-and-social-media

Olmstead, K., Lampe, C., & Ellison, N.B. (2015, June 22). Social media and the workplace. *Pew Research Center*. Retrieved from http://www.pewinternet.org/2016/06/22/social-media-and-the-workplace/

Pagnattaro, M.A. (2004). What do you do when you are not at work?: Limiting the use of off-duty conduct as the basis for adverse employment decisions. *University of Pennsylvania Journal of Labor and Employment Law*, Spring, 625-674.

Pearce, J.A. & Kuhn, D.R. (2003) The legal limits of employees' off-duty privacy rights. *Organizational Dynamics*, *32*(4), 372-383.

Peralta, E. (2011, November 29). Facebook settles with FTC on charges it deceived users on privacy. *National Public Radio*. Retrieved from https://www.npr.org/sections/thetwo-way/2011/11/29/142898301/facebook-settles-with-ftc-on-charges-it-deceived-users-on-privacy

Petrecca, L. (2010, March). Feel like someone's watching? You're right. *USA Today*. ISSN:0734-7456

Privacy in employment. (2013). *Gale Encyclopedia of Everyday Law*. Retrieved from http://link.galegroup.com/apps/doc/CX2760300231/GVRL?u=tel_p_plndc&sid=GVRL&xid=3345ab93

Privacy in the age of the smartphone (2016). *Privacy Rights Clearinghouse*. Retrieved from https://www.privacyrights.org/consumer-guides/privacy-age-smartphone

Riedy, M.K. & Wen, J.H. (2010). Electronic surveillance of Internet access in the American workplace: implications for management. *Information & Communications Technology Law, 19*(1)*,* 87-99.

Roberts, K. (2013, July 9). *Golden Corral food video: Brandon Huber all you can eat ribs YouTube FLA restaurant video goes viral*. ABC Affiliate WFTS Tampa Bay. Retrieved from http://www.abcactionnews.com/news/local-news/water-cooler/report-golden-corral-employee-exposes-florida-restaurant-hiding-food-at-the-dumpster

Roberts, P.W. & Dowling, G.R. (2002). Corporate reputation and sustained superior financial performance. *Strategic Management Journal*, *23*(12), 1077-1093.

Roberts, G. & Sambrook, S. (2014). Social networking and HRD. *Human Resource Development International, 17*(5)*,* 577-587.

Rosenberg, R.S. (1999). The workplace on the verge of the 21st century. *Journal of Business Ethics, 22*(1), 3-14.

Rousseau, D.M. (1995). *Psychological contracts in organizations: Understanding written and unwritten agreements*. Thousand Oaks, CA: Sage Publications.

Satenberg, A.L., Bauman, S.B., Brunswick, A.M., Hudson, E.A., King, S.R., & Levy, S.W. (2016, March) *Employer dodges liability for employee's disparaging social media posts*. Retrieved from http://www.lexology.com/library/detail.aspx?g=068f9d62-9685-415a-b7bc-4342eb069bae

Smith, A. (2015, November 24). Surveillance can uncover FMLA abuse. *Society for Human Resource Management*. Retrieved from https://www.shrm.org/resourcesandtools/legal-and-compliance/employment-law/pages/fmla-abuse.aspx

Smith, W.P., & Kidder, D.L. (2010). You've been tagged! (Then again, maybe not): Employers and Facebook. *Business Horizons*, 53, 491-499. doi:10.1016/j.bushor.2010.04.004

Snyder, J.L. (2010). E-mail privacy in the workplace: A boundary regulation perspective. *International Journal of Business Communication*, *47*(3), 266-294. doi:10.1016/j.bushor.2010.04.004

Social media Fact Sheet. (2017, January 12). *Pew Research Center: Internet & Technology*. Retrieved from http://www.pewinternet.org/fact-sheet/social-media/#

Social networking and reputational risk in the workplace: Deloitte LLP 2009 ethics and workplace survey results (2009). *Deloitte LLP*. Retrieved from http://www.bentley.edu/centers/sites/www.bentley.edu.centers/files/centers/cbe/cbe-external-surveys/social-networking-and-reputational-risk-in-the-workplace.pdf

Solon, O. (2015, August 7). Wearable technology creeps into the workplace. *The Sydney Morning Herald*. Retrieved from https://www.smh.com.au/business/workplace/wearable-technology-creeps-into-the-workplace-20150807-gitzuh.html

Stoughton, J.W., Thompson, L.F., & Meade, A.W. (2013). Examining applicant reactions to the use of social networking websites in pre-employment screening. *Journal of Business and Psychology*, *30*(1), 73-88. doi:10.1007/s10869-013-9333-6

Sydell, L. (2018, March 26). FTC confirms it's investigating Facebook for possible privacy violations. *National Public Radio*. Retrieved from https://www.npr.org/sections/thetwo-way/2018/03/26/597135373/ftc-confirms-its-investigating-facebook-for-possible-privacy-violations

Tabak, F. & Smith, W.P. (2005). Privacy and electronic monitoring in the workplace: A model of managerial cognition and relational trust development. *Employee Responsibilities & Rights Journal*, *17*(3), 173-189. doi:10.1007/s10672-005-6940-z

Thomas, S.L., Rothschild, P.C., & Donegan, C. (2014). Social networking, management responsibilities, and employee rights: The evolving role of social networking in employment decisions. *Employee Responsibilities & Rights Journal*, *27*(4), 173-189. doi:10.1007/s10672-014-9250-5

Totenberg, N. (2010, April 15). Should personal texts from work devices be private? *National Public Radio*. Retrieved from https://www.npr.org/templates/transcript/transcript.php?storyId=125998549

Turban, D.B., & Greening, D.W. (1997). Corporate social performance and organizational attractiveness to prospective employees. *Academy of Management Journal*, *40*(3), 658-672.

Walker, K. (2010). A systematic review of the corporate reputation literature: Definition, measurement, and theory. *Corporate Reputation Review*, *12*(4), 357-387.

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.

When worlds collide: The rise of social media for professional & personal use (2012). *Kelly Global Workforce Index*. Retrieved from https://www.kellyservices.com.au/au/siteassets/australia---kelly-services/uploadedfiles/kelly-kgwi-2-when-worlds-collide-whitepaper.pdf

Whitfield, B.N. (2013). Social media @ work: #policyneeded. *Arkansas Law Review*, *66*(3), 843-878.

Wilkie, D. (2013, July 16). Virtual whistle-blowing: Employees bypass internal channels to expose wrongdoing. Retrieved from http://www.shrm.org/hrdisciplines/employeerelations/articles/pages/virtual-whistle-blowing- bypass-internal-channels-expose-wrongdoing.aspx

Wohlgemuth, J. (2012, August 6). New Jersey District Court denies employer's motion to dismiss plaintiff's cause of action after employee's supervisor gains unauthorized access to employee's Facebook account. *Mondaq Business Briefing*. Retrieved from http://go.galegroup.com.ezproxy.mtsu.edu/ps/i.do?p=ITOF&u=tel_middleten&id=GALE%7CA298849347&v=2.1&it=r&sid=ITOF&asid=e2d13158

Workplace privacy (n.d.). *Electronic Privacy Information Center*. Retrieved from https://epic.org/privacy/workplace/

Workplace privacy and employee monitoring (2017, July 6). *Privacy Rights Clearinghouse*. Retrieved from https://www.privacyrights.org/consumer-guides/workplace-privacy-and-employee-monitoring

Zimmerman, E. (2002). HR must know when employee surveillance crosses the line. *Workforce*, *81*(2), 38-45.

APPENDICES

APPENDIX A: PARTICIPANTS BY SCENARIOS

Participants by Scenario

	Frequency	Percent
Scenario 1	42	10.8
Scenario 2	28	7.2
Scenario 3	31	8.0
Scenario 4	28	7.2
Scenario 5	38	9.8
Scenario 6	36	9.3
Scenario 7	35	9.0
Scenario 8	35	9.0
Scenario 9	33	8.5
Scenario 10	30	7.7
Scenario 11	26	6.7
Scenario 12	27	6.9
Total	389	

APPENDIX B: AGE, GENDER, AND ETHNICITY

Age

	Frequency	Percent
18 - 29	106	27.7
30 - 49	204	52.4
50 - 64	64	16.5
65+	15	3.9
Total	389	

Gender

	Frequency	Percent
Female	210	54.0
Male	179	46.0
Total	389	

Ethnicity

	Frequency	Percent
White; not Hispanic	303	77.9
Black or African American	31	8.0
Asian or Asian American	19	4.9
Hispanic or Latino	23	5.9
American Indian/Native American	1	0.3
Mixed	9	2.3
Other	3	0.8
Total	389	

APPENDIX C: ORGANIZATIONAL DEMOGRAPHICS

Job Level

	Frequency	Percent
Unemployed, seeking employment	7	1.7
Unemployed, not seeking employment	9	2.2
Part-time	81	19.9
Full-time	291	71.5
Student	19	4.7
Total	407	

Note. Multiple responses permitted.

"I am satisfied with my current (or last) boss"

	Frequency	Percent
Strongly Agree	90	23.1
Agree	197	50.6
Neither Agree nor Disagree	48	12.3
Disagree	39	10.0
Strongly Disagree	15	3.9
Total	389	

"I feel loyal to my current (or past) organization"

	Frequency	Percent
Strongly Agree	100	25.7
Agree	164	42.2
Neither Agree nor Disagree	75	19.3
Disagree	35	9.0
Strongly Disagree	15	3.9
Total	389	

APPENDIX D: SOCIAL NETWORK SITE DEMOGRAPHICS

Social Network Sites Visited Most Often

	Frequency	Percent
Facebook	233	59.9
Instagram	55	14.1
Twitter	56	14.4
Other	37	9.5
LinkedIn	7	1.8
Missing	1	0.3
Total	389	

Frequency of Visits to Social Network Sites

	Frequency	Percent
Once a month or less	17	4.4
A few times a month	19	4.9
Once a week	17	4.4
A few times a week	79	20.3
Daily	255	65.6
Missing	2	0.5
Total	389	

Average Time Spent on Social Network Sites

	Frequency	Percent
Less than 10 minutes	88	22.6
10 - 30 minutes	143	36.8
31 - 60 minutes	86	22.1
More than 1 hour but less than 2 hours	43	11.1
More than 2 hours	28	7.2
Missing	1	0.3
Total	389	

Average Scores on Social Media Intensity Scale

	Frequency	Percent
1.00-1.67	144	12.4
2.00-2.67	249	21.4
3.00-3.67	199	17.1
4.00-4.67	440	37.9
5.00	130	11.2
Missing	5	

APPENDIX E: EMPLOYEE MONITORING EXPERIENCE

"Have You Assisted with or Conducted Employee Monitoring in Current/Previous Job?"

	Frequency	Percent
Yes	85	21.9
No	304	78.1
Total	389	

Type of Monitoring

	Frequency	Percent
Surveillance videos	41	22.3
Employee email	33	17.9
Social media sites	86	46.7
Blogs	4	2.2
Other	20	10.9
Total	184	

Note. Multiple responses permitted.

Frequency of Monitoring

	Frequency	Percent
Rarely required in current/previous job	37	43.5
Occasionally required in current/previous job	31	36.5
Frequently required in current/previous job	17	20.0
Total	85	

APPENDIX F: CURRENT EMPLOYEE EXPERIENCES

	Frequency	Percent
Asked to disclose login information		
Yes	18	21.2
No	67	78.8
Asked to disclose browser history		
Yes	14	16.5
No	71	83.5
Fired from a job because of social network site profile		
Yes	10	11.8
No	75	88.2
Friend/family fired because of his/her social network site profile		
Yes	23	27.0
No	62	73.0
Received job offer/promotion because of social network site profile		
Yes	23	27.0
No	62	73.0
More than one Facebook account (e.g. work and personal)		
Yes	19	22.4
No	66	77.6
Think carefully about what to post on social network sites		
Yes	71	83.5
No	14	16.5

Note. N = 85 for all items.

APPENDIX G: QUESTIONNAIRE

Participants were presented with the following welcome letter as it appears with the addition of italicized labels.

Welcome! The purpose of this study is to better understand employees' perceptions of fairness when their employer monitors their social media activity.

Please complete or enter the following before the survey begins:

- Two screening questions to confirm eligibility to participate in this study
- Informed consent agreement
- Your Mechanical Turk worker ID in order to receive payment

Screening Questions
1. What is your age? (e.g. 18) _____
If Greater Than or Equal to 18, then Skip to item 2.
If Less Than 18, then Skip to End of Survey.

2. Do you currently work in the United States?
❍ Yes
❍ No
If No is Selected, then Skip to End of Survey.

INFORMED CONSENT

Study Title: Employees' fairness perceptions of workplace social media monitoring: Privacy invasiveness, smartphone ownership, and work periods
Principal Investigator: Melissa N. McCord
Faculty Advisor: Judith van Hein, PhD
Contact Information: mnm4e@mtmail.mtsu.edu

Dear Survey Participant,

On behalf of the research team, the Middle Tennessee State University (MTSU) would like to thank you for considering to take part in this research study. You have been contacted by the above identified researcher(s) to enroll as a participant in this study because you met its eligibility criteria.

This consent document describes the research study for the purpose of helping you to make an informed decision on whether to participate in this study or not. It provides important information related to this study, possible interventions by the researcher(s) and proposed activities by you. This research has been reviewed by MTSU's internal oversight entity - Institutional Review Board (IRB) - for ethical practices in research (visit www.mtsu.edu/irb for more information).

As a participant, you have the following rights: You should read and understand the information in this document before agreeing to enroll Your participation is absolutely voluntary and the researchers cannot force you to participate If you refuse to participate or to withdraw midway during this study, no penalty or loss of benefits will happen The investigator MUST NOT collect identifiable information from you, such as, name, SSN, and phone number The researcher(s) can only ask you to complete an interview or a survey or similar activities and you must not be asked to perform physical activities or offer medical/psychological intervention Any potential risk or discomforts from this study would be lower than what you would face in your daily life

Part 1 of 4. Please click Next.

Disclosures:

1. What is the purpose of this study?
   The purpose of this study is to better understand employees' perceptions of fairness when their social media is monitored by their employer.

2. What will I be asked to do in this study?
   Participants who meet the qualifications and electronically consent will be asked questions about their opinions and attitudes regarding a fictitious scenario, social

networking site usage, social networking site intensity, experience with monitoring, and demographics.

3. How many times should I participate or for how long?
   You may only complete the survey once. Evidence of multiple attempts will be considered invalid data and will not be included for data analysis. While completing the survey, you can return to previous pages and will not be obligated to complete the survey in one sitting. The survey should take approximately 10 minutes to complete.

4. What are the risks and benefits if I participate?
   All research involves some risk. You are not expected to experience more than minimal risk, which includes a loss of time and potentially some mental fatigue. You will only be asked questions that are not intrusive regarding topics that are not considered inherently sensitive or that would impose on your privacy. You will be able to exit the survey and cancel your responses at any point, up until the moment the survey is submitted. Benefits include $0.75 in compensation through Amazon Mechanical Turk (AMT) and increased knowledge of surveillance practices pertaining to social media and the workplace.

5. What will happen to the information I provide in this study?
   Information will be aggregated and analyzed without any personally identifiable indicators. Subsequent data trends and insights will be included in the researcher's thesis and may potentially be used in future research conferences and/or presentations.

6. What will happen if I refuse to participate and can I withdraw if I change my mind in the middle?
   Participation in this survey is voluntary. There are no penalties for refusal to participate, and participation may be terminated at any time.

7. Whom can I contact to report issues and share my concerns?
   You can contact the researcher(s) by email or telephone (Melissa N. McCord at mnm4e@mtmail.mtsu.edu and Dr. Judith van Hein at judy.vanhein@mtsu.edu or (615) 898-5752. You can also contact the MTSU's Office of Research Compliance by email – irb_information@mtsu.edu. Report compliance breaches and adverse events by dialing (615) 898-2400 or by emailing compliance@mtsu.edu.

Part 2 of 4. Please click Next.

Confidentiality Statement: All efforts, within reason, will be made to keep the personal information in your research record private but total privacy cannot be promised, for example, your information may be shared with the MTSU IRB. In the event of questions or difficulties of any kind during or following participation, you may contact the

Principal Investigator as indicated above. For additional information about giving consent or your rights as a participant in this study, please feel free to contact our Office of Compliance at (615) 898 2400.

Compensation: Participants will receive $0.75 in compensation through Amazon Mechanical Turk (AMT) upon successful completion of the survey.

Study-related Injuries: MTSU will not compensate for study-related injuries.

Exemption Criteria: This study was submitted to the MTSU IRB – an internal oversight entity to oversee research involving human subjects. The IRB has determined that this investigation consists of lower than minimal risk and it is exempt from further IRB processes based on the criteria: "Category 2 - Educational Tests."

Note to the Participant: You do not have to do anything if you decide not to participant in this study. But if wish to enroll as a participant, please complete the next part of this informed consent form. Please retain a copy of the informed consent for your future reference.

Part 3 of 4. Please click Next.

You have been contacted because the researcher believes you meet the eligibility criteria to participate in the above referenced research study. Be aware that you must NOT be asked by the researcher to do anything that would pose risk to your health or welfare, such as:

- Identifiable information – name, phone number, SSN, address, College ID, social media credentials (Facebook page, Twitter, etc.), email, identifiable information of closest relatives and etc.
- Physical activities – like exercise studies Medical intervention – testing drugs, collection of blood/tissue samples or psychological questions
- Nothing risky – any proposed activity that would expose you to more risk than what you would face on a day to day basis is not approved by the IRB.

However, you can do the following:

- Withdraw from the study at any time without penalties (Please note, participants will receive $0.75 in compensation through Amazon Mechanical Turk (AMT) upon successful completion of the survey)
- Withdraw the information you have provided to the investigators before the study is complete
- Ask the researcher questions about the procedures used in the research.

Part 4 of 4. Please click Next.

I have read the informed consent for the identified research. I understand what to expect from the online survey and my questions have been answered.

By clicking Agree, I give my consent to participate in this study. Click Decline to exit the survey.

❍ Agree
❍ Decline
If Decline is Selected, then Skip to End of Survey.

MTurk Worker ID
Please enter your Mechanical Turk worker ID. It is very important you enter this correctly or payment cannot be made. If you have already completed this study on an earlier HIT, you cannot complete it again.

Mechanical Turk Worker ID: _____

Scenarios

Participants read one randomly assigned scenario (items 3-14) and selected his or her level of agreement.
Question Randomization: Present only 1 of total questions.

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
The monitoring practice is fair to the employee.	❍	❍	❍	❍	❍
The employer's decision to monitor employees is justified.	❍	❍	❍	❍	❍
Terminating this employee based on this monitoring practice is justified.	❍	❍	❍	❍	❍

Scenario 1

Privacy invasiveness	Work Period	Smartphone Ownership
Low (boss does a public search)	Off-duty (authorized break)	Low (personal)

Taste of Beans Co. is a popular global American coffee company and retail coffeehouse chain. One day during a short off-duty break, an employee named Corie took out their personal smartphone and posted the following to Facebook:

our customers would flip if they knew we toss recyclables in the same dumpster as the trash. world's most ethical company my ass! #TasteofBeansCo

Corie's boss monitors employees' social media activity by doing general public searches online. The boss found the social media post and then fired Corie.

Please select your level of agreement about the scenario.

Scenario 2

Privacy invasiveness	Work Period	Smartphone Ownership
Low (boss does a public search)	On-duty (unauthorized break)	Low (personal)

Taste of Beans Co. is a popular global American coffee company and retail coffeehouse chain. One day during a shift, an employee named Corie took out their personal smartphone and posted the following to Facebook:

our customers would flip if they knew we toss recyclables in the same dumpster as the trash. world's most ethical company my ass! # TasteofBeansCo

Corie's boss monitors employees' social media activity by doing general public searches online. The supervisor found the social media post and then fired Corie.

Please select your level of agreement about the scenario.

Scenario 3

Privacy invasiveness	Work Period	Smartphone Ownership
Medium (coworker shows boss)	Off-duty (authorized break)	Low (personal)

Taste of Beans Co. is a popular global American coffee company and retail coffeehouse chain. One day during a short off-duty break, an employee named Corie took out their personal smartphone and posted the following to Facebook:

our customers would flip if they knew we toss recyclables in the same dumpster as the trash. world's most ethical company my ass! #TasteofBeansCo

Corie's coworker and Facebook friend, Jordan, saw the post. Jordan showed the social media post to their boss, who then fired Corie.

Please select your level of agreement about the scenario.

Scenario 4

Privacy invasiveness	Work Period	Smartphone Ownership
Medium (coworker shows boss)	On-duty (unauthorized break)	Low (personal)

Taste of Beans Co. is a popular global American coffee company and retail coffeehouse chain. One day during a shift, an employee named Corie took out their personal smartphone and posted the following to Facebook:

our customers would flip if they knew we toss recyclables in the same dumpster as the trash. world's most ethical company my ass! #TasteofBeansCo

Corie's coworker and Facebook friend, Jordan, saw the post. Jordan showed the social media post to their boss, who then fired Corie.

Please select your level of agreement about the scenario.

Scenario 5

Privacy invasiveness	Work Period	Smartphone Ownership
High (software alerts boss)	Off-duty (authorized break)	Low (personal)

Taste of Beans Co. is a popular global American coffee company and retail coffeehouse chain. One day during a short off-duty break, an employee named Corie took out their personal smartphone and posted the following to Facebook:

our customers would flip if they knew we toss recyclables in the same dumpster as the trash. world's most ethical company my ass! #TasteofBeans

Corie's boss uses surveillance software that electronically monitors employees' social media activity. When the software alerted the boss about Corie's social media post, the boss fired Corie.

Please select your level of agreement about the scenario.

Scenario 6

Privacy invasiveness	Work Period	Smartphone Ownership
High (software alerts boss)	On-duty (unauthorized break)	Low (personal)

Taste of Beans Co. is a popular global American coffee company and retail coffeehouse chain. One day during a shift, an employee named Corie took out their personal smartphone and posted the following to Facebook:

our customers would flip if they knew we toss recyclables in the same dumpster as the trash. world's most ethical company my ass! #TasteofBeansCo

Corie's boss uses surveillance software that electronically monitors employees' social media activity. When the software alerted the boss about Corie's social media post, the boss fired Corie.

Please select your level of agreement about the scenario.

Scenario 7

Privacy invasiveness	Work Period	Smartphone Ownership
Low (boss does a public search)	Off-duty (authorized break)	High (work-issued)

Taste of Beans Co. is a popular global American coffee company and retail coffeehouse chain. One day during a short off-duty break, an employee named Corie took out their work-issued smartphone and posted the following to Facebook:

our customers would flip if they knew we toss recyclables in the same dumpster as the trash. world's most ethical company my ass! #TasteofBeansCo

Corie's boss monitors employees' social media activity by doing general public searches online. The boss found the social media post and then fired Corie.

Please select your level of agreement about the scenario.

Scenario 8

Privacy invasiveness	Work Period	Smartphone Ownership
Low (boss does a public search)	On-duty (unauthorized break)	High (work-issued)

Taste of Beans Co. is a popular global American coffee company and retail coffeehouse chain. One day during a shift, an employee named Corie took out their work-issued smartphone and posted the following to Facebook:

our customers would flip if they knew we toss recyclables in the same dumpster as the trash. world's most ethical company my ass! #TasteofBeansCo

Corie's boss monitors employees' social media activity by doing general public searches online. The supervisor found the social media post and then fired Corie.

Please select your level of agreement about the scenario.

Scenario 9

Privacy invasiveness	Work Period	Smartphone Ownership
Medium (coworker shows boss)	Off-duty (authorized break)	High (work-issued)

Taste of Beans Co. is a popular global American coffee company and retail coffeehouse chain. One day during a short off-duty break, an employee named Corie took out their work-issued smartphone and posted the following to Facebook:

our customers would flip if they knew we toss recyclables in the same dumpster as the trash. world's most ethical company my ass! # TasteofBeansCo

Corie's coworker and Facebook friend, Jordan, saw the post. Jordan showed the social media post to their boss, who then fired Corie.

Please select your level of agreement about the scenario.

Scenario 10

Privacy invasiveness	Work Period	Smartphone Ownership
Medium (coworker shows boss)	On-duty (unauthorized break)	High (work-issued)

Taste of Beans Co. is a popular global American coffee company and retail coffeehouse chain. One day during a shift, an employee named Corie took out their work-issued smartphone and posted the following to Facebook:

our customers would flip if they knew we toss recyclables in the same dumpster as the trash. world's most ethical company my ass! # TasteofBeansCo

Corie's coworker and Facebook friend, Jordan, saw the post. Jordan showed the social media post to their boss, who then fired Corie.

Please select your level of agreement about the scenario.

Scenario 11

Privacy invasiveness	Work Period	Smartphone Ownership
High (software alerts boss)	Off-duty (authorized break)	High (work-issued)

Taste of Beans Co. is a popular global American coffee company and retail coffeehouse chain. One day during a short off-duty break, an employee named Corie took out their work-issued smartphone and posted the following to Facebook:

our customers would flip if they knew we toss recyclables in the same dumpster as the trash. world's most ethical company my ass! # TasteofBeansCo

Corie's boss uses surveillance software that electronically monitors employees' social media activity. When the software alerted the boss about Corie's social media post, the boss fired Corie.

Please select your level of agreement about the scenario.

Scenario 12

Privacy invasiveness	Work Period	Smartphone Ownership
High (software alerts boss)	On-duty (unauthorized break)	High (work-issued)

Taste of Beans Co. is a popular global American coffee company and retail coffeehouse chain. One day during a shift, an employee named Corie took out their work-issued smartphone and posted the following to Facebook:

our customers would flip if they knew we toss recyclables in the same dumpster as the trash. world's most ethical company my ass! # TasteofBeansCo

Corie's boss uses surveillance software that electronically monitors employees' social media activity. When the software alerted the boss about Corie's social media post, the boss fired Corie.

Please select your level of agreement about the scenario.

Open-Ended Comment
15. Why did you react that way? Please be as specific as possible.

Attention Checks
16. The current year is 2018.
❍ Agree
❍ Disagree
Randomize the order of all questions.
See item 41 for the second attention check.

Social Network Site Usage
17. Do you have personal social media account(s)?
❍ Yes
❍ No

18. Which social media platforms do you have a personal account(s)? (Check all that apply.)
❏ Facebook
❏ Twitter
❏ LinkedIn
❏ Instagram
❏ Pinterest
❏ Snapchat
❏ Tumblr
❏ WhatsApp
❏ YouTube
❏ Other (allow text entry)

19. How often do you check social media?
❍ Once a month or less
❍ A few times a month
❍ Once a week

❍ A few times a week
❍ Daily

20. If you had to choose, which social media platform do you visit most frequently?
❍ Facebook
❍ Twitter
❍ LinkedIn
❍ Instagram
❍ Other (allow text entry)

21. How much time do you typically spend using the social media platform you visit most frequently?
❍ Less than 10 minutes
❍ 10 – 30 minutes
❍ 31 – 60 minutes
❍ More than 1 hour but less than 2 hours
❍ More than 2 hours

Social Network Site Intensity
Please select your level of agreement for the following statements about your social media usage. *(items 22-24)*

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
I feel out of touch when I have not logged onto social media for a while.	❍	❍	❍	❍	❍
I feel I am part of social media communities.	❍	❍	❍	❍	❍
I would be sorry if social media sites were shut down.	❍	❍	❍	❍	❍

Experience with Monitoring
25. Have you ever assisted with or conducted employee monitoring in your current or previous job?
❍ Yes
❍ No
If No is Selected, then skip to End of Block.

26. Please select which type(s) of employee monitoring you have either assisted with or conducted? (Check all that apply.)
❑ Surveillance videos
❑ Email screening

❑ Social media site screening
❑ Blogs
❑ Other (allow text entry)

27. How often does your current or previous job require you to monitor current employees?
❍ Employee monitoring is rarely required in my current/previous job
❍ Employee monitoring is occasionally required in my current/previous job
❍ Employee monitoring is frequently required in my current/previous job

Please select a response to the following statements about your experiences. *(items 28-34)*

	Yes	No
Have you been asked to disclose your login information to an employer?	❍	❍
Have you been asked to disclose your browser history to an employer?	❍	❍
Do you believe you have been fired from a job because of information an employer found on your social media profile(s)?	❍	❍
Do you believe a friend or family member has been fired from a job based on information an employer found on his/her social media profile(s)?	❍	❍
Do you believe you received a job or a promotion because of your social media profile(s)?	❍	❍
Do you have more than one Facebook account (e.g. profile for work and a private profile for family and friends)?	❍	❍
Do you carefully think about what you post on social media?	❍	❍

Participant Demographics
35. What is your age?
❍ 18 – 29
❍ 30 – 49
❍ 50 – 64
❍ 65+

36. Which best describes you?
❍ Male
❍ Female

37. 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

Organizational Demographics
38. What is your job level? (Check all that apply.)
❑ Unemployed, not seeking employment
❑ Unemployed, seeking employment
❑ Part-time employee
❑ Full-time employee
❑ Student

Please select your level of agreement with the following statements about your organization. *(items 39-41)*

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
"I am satisfied with my current boss" (or "I was satisfied with my last boss" if unemployed)	❍	❍	❍	❍	❍
"I feel loyal to my current organization" (or "I felt loyal to my past organization" if unemployed)	❍	❍	❍	❍	❍
For quality assurance purposes, please select "Agree".	❍	❍	❍	❍	❍

412Please select the industry that best describes your organization.
❍ Business/Professional Services
❍ Financial Services
❍ Government
❍ Manufacturing
❍ Public Administration
❍ Wholesale/Retail
❍ Education
❍ Other (allow text entry)

Debriefing Questions

You are nearly finished. Your responses to these next questions will NOT influence your payment for this study. Please answer honestly.

43. Did you take this study seriously, or did you click through the responses?
❍ Just clicked through
❍ Took the study seriously

44. Is there any reason why we should NOT use your data?
❍ My data should NOT be included in your analyses
❍ My data should be included in your analyses

45. Why should we NOT include your data in our analyses?
❍ I wasn't really paying attention
❍ I just clicked randomly
❍ I didn't understand the task/questions
❍ I didn't really know what I was doing
❍ I just skimmed through the questions
❍ Other _____

46. Finally, what do you think is the purpose of this study? _____

Thank you for your participation. Your response has been recorded. If you have questions or would like to know the results of this study, please contact Melissa N. McCord at mnm4e@mtmail.mtsu.edu.

Your MTurk survey code is ${e://Field/mTurkCode}

Thank you for your participation. Enter the following code on the Mechanical Turk website to verify that you completed the survey.

APPENDIX H: CORRELATIONS

	Employee Monitoring Experience	Age	Gender	Job Level	Social Network Site Intensity
Employee Monitoring Experience	-				
Age	-.071	-			
Gender	-.073	,069	-		
Job Level	.162**	-.152**	-.246**	-	
Social Network Site Intensity	.031	-.063	-.207**	.022	-

Note. Gender coded: female = 1, male = 0.
**. Correlation is significant at the 0.01 level (2-tailed).
*. Correlation is significant at the 0.05 level (2-tailed).

APPENDIX I: SCALE RELIABILITY

Personal Smartphone Scales Reliability

Scenario	Variables	Cronbach's Alpha	Cronbach's Alpha if "Terminating Employee" Item Removed
1	Public Search, Authorized Break (off-duty)	.866	.845
2	Public Search, Unauthorized Break (on-duty)	.914	.846
3	Coworker, Authorized Break (off-duty)	.847	.874
4	Coworker, Unauthorized Break (on-duty)	.927	.923
5	Monitoring Software, Authorized Break (off-duty)	.937	.941
6	Monitoring Software, Unauthorized Break (on-duty)	.892	.863

Work-Issued Smartphone Scales Reliability

Scenario	Variables	Cronbach's Alpha	Cronbach's Alpha if "Terminating Employee" Item Removed
7	Public Search, Authorized Break (off-duty)	.908	.897
8	Public Search, Unauthorized Break (on-duty)	.889	.930
9	Coworker, Authorized Break (off-duty)	.884	.834
10	Coworker, Unauthorized Break (on-duty)	.808	.785
11	Monitoring Software, Authorized Break (off-duty)	.957	.898
12	Monitoring Software, Unauthorized Break (on-duty)	.885	.896

APPENDIX J: QUALITATIVE COMMENTS

I feel that no one has the right to tell you what you can and can't do when it comes to your social media posts. The fact that the employee posted the comment when she was on the clock, however, may be justified if it was previously stated to all employees that this monitoring was being done. I worked for an organization that made all the employees sign a form that we would not post anything bad about the organization on social media at the risk of "disciplinary action". We all felt this was wrong but we were warned ahead of time so we knew what was at stake.
if he thinks is job isn't fair he should quit and then express his opinion

---

I feel like you should be held responsible for things you say but i also feel like work shouldn't be looking through your personal social media. Also I feel that people need to be aware of what's public online.

I don't think it's appropriate for employers to monitor employees' social media activity.

I think the individual posting comments on social media should have posted something positive about the workplace instead of posting something negative. As the phrase goes "If you can't say something nice then don't say anything at all." The worker should already know to not put anything that puts the company down on social media.

---

it is unethical what the company is doing

I do not know what is written in their contract and work policy. If it is clearly stated there that employees are being watched and not allowed to badmouth their employer, and Corie signed the contract, then it is foolish of her to behave like this.

The employee was using social media during his work hours, and directly referred to the company in public

---

I work for an employer that allows use of social media while working. I think if you are irresponsible enough to say bad things about the company you work for, you deserve to face repercussions. Not only that, but he was not vague or ambiguous about who his employer was and even hashtagged the company in his post. All of his actions were done in poor taste.
Well it was a work issued smart phone so I think the company has the right to monitor the content it posts. I would wonder whether the employee was notified but really even that is not much of an excuse in this day and age.

I think that the monitoring of employees is not correct

It is unethical to post a negative status about your place of employment.

Well you should not be posting negative items about your company and expect everything will be fine. The company has a brand to protect.

I find it repulsive to have a social media clause in any employment agreement. However, if one is constrained by such, one must abide by that policy. Hence, the firing was rightfully so, but the policy itself is distasteful.

It's common sense to not publicly bash the company one work's for. The employee could have presented her concerns and a proposition on how to fix it to her employer and potentially elevated herself in the company. Do stupid things, win stupid prizes.

Because if he has an issue with the company he should talk to his management, HR or use some whistle blower line which every company has established. You can't post about your company on social media without any consequences.

There are privacy settings on FB for a reason. The employer was doing a search of public posts and came across this from his employee. He has the right to be concerned about public perception of his business. I think he could have handled it with a warning before resorting to dismissal. She could have avoided the entire situation by being more discerning about her choice of posts.

The employee's post could be seen as potentially damaging to the company's reputation, thereby affecting sales and profits. Also, the individual that was fired was not being paid to use his phone, for either good or bad comments. That alone would be grounds for termination, in my estimation.

I thought it should be taken very seriously because the post was very specific about which company the employee was referring to. If it had been more generic I don't think it would have been a major issue.

The employee should not be sharing private company practices on social media, and criticizing her employer like that is bad for reputation.

Everyone has an opinion to share, just because it is negative firing an employee is wrong. And i believe monitoring an employees social media activity sounds really like stalking. That person is employed there and has her rights as well.

Because it was a company phone

Corie is the image of the company and should have been professional

---

I hate the idea of employers monitoring their employees social media accounts. I think it is just wrong. That said, what an incredibly dumb move on this employee to not only post such an awful swipe about her place of employment in a public platform such as Facebook but to do it on their work issued phone. I would not have only fired this person,

I would have sued them for going against (what I am assuming the company required) their NDA.

She has made public a complaint, which is pretty severe in the company's eyes, about the company's integrity and the boss's integrity. Though it may be true that they don't recycle and not recycling is not against the law, it has put the company's reputation in a bad light. It's best to fire Corie to also show an example to others, even though it seems harsh. Once it's posted, it's too late to take it back, even if it's deleted.

If an employee acted in a way that put customers off in the workplace, that employee wouldn't be there for long. That would be grounds for termination. So why would it be any different online? If an employee is posting things online that put customers off, that hurts the company, too. Employees shouldn't expect the company to keep them when they're doing things that hurt the company. They should be told when they're hired that posting negative things about the company online is not acceptable and may very well lead to termination. In this particular case, however, the employer might not have ever had that conversation with this employee. If that's the case, then I think the employer should have that conversation now, reprimand the employee, but give her a second chance.

An employee should retain their right to privacy and free speech without being monitored for non-work-related behavior that may be deemed unsavory. At the same time, however, the employee presumably knew of the monitoring and still chose to make disparaging comments about the company, using a company-owned phone no less, on a public forum. For actions that directly damage a company's image or customer base, it makes complete sense that they would be reprimanded. Direct monitoring and punishment for inconsequential things is definitely unfair, but actions do also have consequences.

The employee should not paint his/her company is a negative limelight.

First, the phone was issued by the company so it technically doesn't belong to the user. Second, they disclosed company information across the internet through social media. That in itself is grounds for termination.

I would need to know if the employee had some kind of problem with the company and/or manager, and wanted to get back at the company and/or manager, or if she was truly concerned about the ecological impact of trash and recyclables as it relates to that company/location. I would need to investigate and see if the story on social media was true, exaggerated, made up, and/or company-wide or limited to the one location. There is simply not enough information for me to make an informed decision.

You have to expect some repercussion from posting something negative. Especially since the company issued the cell phone.

The employees actions could have very well put the company's reputation and well being in jeopardy so I can see why the employer fired him. However, I don't think it's fair to spy on employees, what they do in their free time is their business and he also spoke on a issue that many supporting customers would want to know about. The company is basically operating under a lie. I think the employee should have considered whether or not the company he worked for aligned with his own beliefs and values and quit if the company wasn't a match. All in all it was time for the employee to part ways with the company anyway.

The employee is defacing the company, regardless of if her claim has basis. She could have taken a proactive, constructive route instead.

I think the manager was right to fire. It is not okay for an employee to make such a derogatory tweet about the company, especially while at work and using company property. I would be very upset with and disappointed in this employee

---

I'm in the middle on this one. I believe that you should always keep your work life off of a social media. On the other hand, if you are aware of the circumstances and feel you should be "heard" about certain situations, then post away. I don't think the employee should've been fired, more as, given a warning instead and fix the problem the employee was stating.

Because the employee posted the information online knowing that their employer would see it
The business is within its rights to surveil. The business is probably within its rights to terminate employment in this situation. The extent to which standards were communicated to the employee is unclear. This makes the employee's action a little harder to judge. Is the business engaged in false advertising or fraud concerning its practices, or is it simply engaged in nominal advertising hyperbole (which courts have held to be legal and harmless)? This question is unanswered.
this was a work issues phone, so there is probably an agreement for behavior similar to appropriate behavior in the workplace. However, the boss looking around on google for public posts, rather than identifying what has been done directly through the phone's history, points at a slight violation of privacy.

The monitoring of social media posting can have two business related functions which makes it acceptable in my view. The first is a quality control check for any posts which the company wants posted. The second reason is to check for unauthorized postings on company time. Unless on a break or allowed otherwise, social media use should be for business reasons only during work.

---

1. She accessed her personal social media account during work hours. 2. She publicly denigrated her employer. 3. The information she posted was visible by anyone. Her employer did not illegally access her personal/confidential information. Therefore,

regardless of whether not a confidentiality agreement was in place, as a common-sense matter, her employer had every right to terminate her.

He had an opinion and stated it on facebook. He didnt do it to "destroy" the company. He just talked about the trash not about food violations.

When you are being paid and on work hours you should stay off of social media. Your personal stuff should stay at after work hours. Never post bad comments about your company that's not smart.

It was unfair to the employee to be fired for stating the truth.

I do not think his actions were work related. I do not believe in firing someone for posting information on social media. If his phone was a work phone that his employer pays for then I believe he should have been fired. The company supplied phone is for work not personal us.
One employee can destroy a business, even if the accusation is true. The business however, should have it clearly outlined in the work contract that this behavior is not allowed. There should be a way to inform the bosses without going to social media.

She posted it using a company phone. Also, it was negative company info that an employee leaked to the public.

I would have to see the employee employer signed contract before making a definitive decision
Well, I don't agree with the policy, but as long as the policy was disclosed before he was hired, it is fair game.

The employee is not authorized to publish information about the employer (unless they are designated as such). The company is free to share or not share information with the public, and Corie decided to share information about the company's operations.

We have too many eyes in our business already

Had the employee done an equivalent deed in the physical world, he or she might have done something like wear a sandwich board outside the coffee company with a message such as the one she wrote on social media. By choosing to express sentiments and opinions on social media, one is making a public statement not protected by a right of privacy. Notice that many social media platforms allow one to keep certain posts and statements private: The employee should have submitted her post using one of those privacy features.

Just cant think of any other possible solutions.

The loyalty of an employee is important. there is always someone else that would like the job.

Because you should have a duty to your work company and not bad mouth them. If Corie felt that way he should have talked to management and tried to implement a recycle policy.

Because even if its social media and he can monitor the activity doesn't mean anyone should be fired for stating there opinion. That being said the employee shouldn't be taking out there phone to post things unless on a break or a lunch. If the employee is on one of those then its none of the Bosses business what you post. You should be allowed to express yourself.

Negative comments on social media should never be directed toward your employer. The old saying "never bite the hand that feeds you" comes to mind.
The worker Corie should've never taken to social media and expressed the distaste / put down on the company the way they did. Saying "world's most ethical company my ass" is most likely the reason they lost their job.

Doing non-work things while on the clock at work is not part of doing one's job. It's extracurricular and should not be done during work hours.

Such overt and gratuitous disrespect by an employee to an employer in a public forum is unacceptable. There are more productive ways to raise those concerns if they are legitimate.
I think it's not right to criticize your employer on social media.

Because of corey should entitled to say what he wants on his social media account. As long as his post is not hurtful to other people or harming them.

One's life outside of work is private and separate from the organization they work for. If the employee were to do something wrong in person while on duty, then firing him would be justified. However, firing him for expression in a medium outside of work is unjustified.
I considered what should have happened. The employee should have gotten in connection with the company and created some high-profile positive message to get the eco-problem turning into a super win. So, her method was wrong. The Boss, looking at social activity can do whatever he wants since it is pubic information. The employee knew better; had to know better than to post and think it would not get back to her.

An employer has a right to monitor employees

I think monitoring is fair, but it outcome should not limit one's 1st Amendment right of expression

---

I believe the employee did not say anything very controversial enough to have them terminated. The employee could have handled the situation differently by suggesting the company start to recycle, but I do not think posting this on social media is grounds for firing him. I also disagree with employers using software to monitor their employees activity on social media. This is an invasion of their privacy.

I think people are entitled to say what they think, but you have to remember to ask yourself if it's going to affect your employment. Our bosses already told us and it's now in the employee handbook, don't mention your job on Facebook or face being fired. I don't think it's fair. I think maybe they should be warned first, then if it happens again, then fire them. Some people don't really care though. I've noticed the younger population seems to feel more free to post their feelings. Us older people watch more careful.

The employee used a company issued phone and company hashtag , under which I support the monitoring of the social networking activity.

I don't feel like bashing your employer on social media is the right thing to do. Although, I do believe that there should be a social media clause stating this in an employee handbook so that they have the right to fire a person for this kind of violation.

You dont use a company phone to post on social meadow talking bad about your company
She's mentioning the place she works for, and then slagging them in public. Can't happen. On the way hand I'm not fond of employers monitoring that kind of activity. Even though the information is public, it seems a bit invasive. That being said, the information posted is controversial and not something to be published in that manner. If he/she had a problem with it, there are other ways to bring the matter up.

The post reflects badly on the company and damaging their business. The employer has the legal rights to fire the employee.

I reacted the way I did because the employees comment was very unprofessional and very bad for business.

I don't think it was appropriate of her to post that but I think what the employee does on her own time is really her own business.

The employee should be free to express her opinions, even if she did it in an unprofessional manner.

Nobody has the right to monitor people personal lives. If he has an opinion and he posted online then that is not a justification to fire him. I am completely against it.
If the company has a formal written policy that specifically prohibits employees from posting negative information the company then the employee's firing was justified. If

there is no policy against making negative posts about the company ... then the company is not justified in firing the employee.

Social media is a way for individuals to express themselves. I don't think it should be monitored closely, but the post the employee made was very unethical especially since the individual represents the company.

The employee chose to use an easily searched hashtag

I believe that whistleblowing is an important thing, whether or not it is against the company policy. I still think a company is in the right for firing an employee for badmouthing the company, but it still should have taken into account what the employee was talking about as a solid point insulting their supposed image.

I don't think that employers should monitor employees social media. If the employer has a monitoring policy, then the employees should be aware.

Employees shouldn't post about items without trying to solve the problem first. it shows the person is immature.
I do believe that posting negative information about your workplace to social media is damaging to the company and also reflects badly on your image as an employee.
I think it's fair to monitor the employees on things that they post publicly. However, I don't think it was fair to fire her based on what she posted. What she posted was the company's own fault and she was looking out for the greater good posting it.

Posting on social media is purely a personal affair and shouldn't be monitored by employers. Plus what the employee said on social media about the company is true.

Using software to specifically monitor employees' social media is an inexcusably Orwellian practice and firing anyone on this basis is autocratic. However, the employee DID specifically tag the company in her post, so if her superiors at the company had simply noticed the company had been tagged in a defamatory post and fired her for it that would be totally justified. It's the surveillance specifically that I take issue with.

I feel that an employee having a difference of opinion with the employer is not reason to justify being fired. It's not like they stole something or kept calling in sick or coming in late or weren't doing their job.

---

i feel that there is a privacy issue if the manager would have said no cell phones and the employee did not follow the rules then yes they should have been fired. but then that should be the rule of all employees no cell phones allowed in work areas while working your shift.

ITS THE RIGHTS TO KNOW WHAT EMPLOYESS ARE SAYING ABOUT THE STORE

Honestly, it's a slippery slope. On the one hand, using the company name and posting something anathema to it's core mission statement is very damaging to the company's reputation and possible profit. Therefore, firing the employee is obviously justified. However, monitoring personal posts is intrusive and sets a standard of interference that might open the door to other, not as justified situations. I am uncertain in this case of which is the better path. That it was on work time and the name of the company used makes me fall a little further on the side of the employer.

Because when people are at work, they should be working, not posting on social media. However, I feel that being fired may have been harsh.Maybe the supervisor could have given the person a warning first.

Company provided the phone so there was no expectation of privacy. As a company phone, regardless of whose possession it is in, it is meant to be used for company business. She disparaged the company she worked for and if those were her feelings, then good bye and good luck.

If we allow employers to monitor employees like that and take away their livelihood over valid statements, it's a mark against free speech. People need to be able to have free lives outside of work

---

Most employees are terminable at will for any or no reason. The disparagement of the company is sufficient reason (although unnecessary) for the firing.

Because the comment of the employee about the company he is working some very strong. Even though, when you don't like what you're seeing about the company, the employee supposes to be loyal to his employeer.

Because at times when we take jobs we accept certain rules. If they agreed to have their Facebook monitored then it was legitimate that they did. Not only that but he did it on a phone provided by the company.

Seemed appropriate

The way also good because the way also different peoples are walking those people are walking that way they also highly talented people that can be social media also will be provide to that way

---

it was based on my principals

I'm assuming you mean 'monitoring' as in the boss read the post when it was brought to their attention. Putting information out into the public sphere that could be damaging to the company is definitely a fireable offense. I would not agree with a company continuously monitoring employee accounts, especially if they are private.

They were mad that their company's true side was revealed, assuming the information presented is true. Or if it was false, firing for falsified information. But either way, social media is really not an employer's place to monitor or spy on employees due to the confidentiality of an employee's private life. In retaliation, they could have proven they did recycle. It almost seems like they are making a statement and proving they don't recycle.

Because I believe employees need to be aware of what they are posting on their social media about their job, family, etc. I believe employees should not post anything related to their job on social media on the first place. That is why I think firing the employee was justified.
I feel that it is unfair to monitor employees in this way anyway. It is a total invasion of privacy. To fire her due to an unjust practice is unfair

---

The employee is creating a negative image of the organization, one that he is personally profiting from.

A) It was a work issued phone B) It was done during work hours. C) I assume it is an "at will" employment relationship. So, even if A and B were not true, she can be fired for C. But she hit the trifecta.

The employee should have never done that regardless of the process they go through. They should limit that kind of social interference.

---

because although i believe in workers rights i also believe that the people who run the company also have rights, and if an employee were to post disparaging comments or company secrets on social media then that employee could be terminated for those posts.

IT IS NOT FAIR TO FIRE AN EMPLOYEE BASED ON SOCIAL MEDIA IF THEY ARE A GOOD EMPLOYEE SOME PEOPLE POST STUPID STUFF ON SOCIAL MEDIA WITHOUT THINKING AND IF YOUR A GOOD EMPLOYEE THAT SHOULDN'T COUNT AGAINST YOU ESPECIALLY IF IT HAS NOTHING TO DO WITH YOUR JOB

Because although the company's actions are wrong. An employer should not put that out to light in social media while in work. If there was an issue with this situation, its best to work it out in private.

It is up to the company to protect itself.

The smartphone that Corie used to post on her social media page was her work-issued phone.

That is technically the property of the company and I believe they should be allowed to monitor her social media through that device. Her posting was detrimental to the company image.

They should hold them responsible for endangering the environment especially being a very reputible coffee company. They need to hold the standards higher and punish individuals who fail to do so.

I don't think employers have the right to monitor employees social media accounts. Now they do have a say so on what an employee does during work time and can put rules in for that. Also, if an employee says negative things on social media about their employer and they find out then they can take action.

Monitoring employee social media on company time is totally appropriate. Even if they are on their own personal equipment. The employees actions were insubordinate and deserves action. However, monitoring social media when the employee is not on company time is not appropriate. The employee regardless was stupid, the employer may have overstepped their bounds. In this particular case, employee termination was appropriate. If the activity was done on private time and the organization was made aware of it, without monitoring, termination may not be appropriate but discussing the issues with the employee may have been better.

The employee posted a negative comment which in turn could affect the company.

I do not think what the employer did was right. The employees need to be aware that the employer is monitoring their posts. The employer should also let them know that the expectation of privacy is very limited when posting on the job. The policy should state something about posting any negative things about the company would be a violation that could result in a firing.
The employee posted the comment on a public social media platform. Therefore, she has no right to privacy from her boss. Firing her made sense since she exposed something harmful about the company.

I think it's an invasion of privacy. I think it breaks down trust between employees. Employees should not be monitoring each other and ratting each other out to the boss. If the company wants to have a strict social media policy, let them police it themselves.

---

used work issued phone for one thing. i would want my employees to be enthusiastic about working at my chain. even though she has a good complaint she should speak to the manager instead of what she did.

Generally, I hate the idea of employers monitoring their employee's social media but I think this situation was different. I think it was justified because Corie was making public statements about the company. It was different than if Corie's boss just disapproved of his lifestyle choices or political statements.

They knew that throwing out recyclable material was wrong, especially when the company has an active campaign to be a green company.

The fact of the matter is that she used the company phone. What world is it ok to talk bad about your employer via their own equipment? If she had rather done this on her own accord using her own devices it would be a little more acceptable. Even then, why would she continue to work at a place that she seems so disgusted with? Why not use tactful means to ask the managers if they could start recycling. She deserved to be fired 100%

I think that a person is entitled to their opinions even if it was in reference to their employer. It was merely her opinion. I think that she shouldn't have done it and that if it was seen by her employer then they do have the right to terminate her for the offense if they wish. I wouldn't have done so - I would have talked to her about her concerns and see if we could do something about them.

Because, you can't bash the company that you work for online, when God knows how many people will see it. It's just very disloyal, and it could have terrible consequences for the business.
In this case, the company was reacting to his whistle blowing post. In this instance, it would be unethical to fire him over this. Most companies have a social media policy in place to keep visible employees from posting things that are their own opinions but may be misconstrued as the company's beliefs.

It is totally wrong for an employee to write derogatory information about a company on social media. If a company has unethical it should be reported to a consumer protection or other responsible agency.

---

too much monitoring may be good in some ways but negatives outweigh them

---

Employees should definitely not talk in a negative way about their employer. It is their employer's prerogative to fire an employee that might cost them business.

I don't think it's right for companies to be able to monitor employees social media. I think it's a breach of privacy.

Saying anything bad about your employer would be considered derogatory and be grounds for termination

---

Employees are being paid for some amount of loyalty to their employer. Her pairing this while at work made it even worse. If I called out my work On social media im this way and my employer saw it I would be reprimanded if not fired. This isnt whistle blowing. This is sharing an opinion that is negative about an employer in a public forum.

The employee used the company's phone to post a comment degrading the company. They should have been fired.

I don't think the employee should have posted that on social media, especially publicly. However, I also don't think the employer should use surveillance software. I would much rather see trust in workers and company's living up to their ethical values (recycling, in this case).
As long as the the surveillance of employees and their social media use is disclosed to employees than I view the policy as fine. If the policy is being enacted without employee knowledge than I do not agree with it.

---

you can not say things about the company you work for on social media. It is plain and simple. You shouldn't even say positive things.

He did it on a company issued phone and hashtagged the company. I would have fired his as% too!

The action on social media causes a negative effect on the image of our company and can not be tolerated.

It is just a big toss up in my everyone deserves to have a private life that is totally separate from their work life and work should just let them.Then on the other hand every company deserves to make sure that people don't say anything wrong about them.

The manager was only accessing open and public information, there is nothing wrong with that. Employees should not post negative information (this information might have a negative impact on the business) online, and to be honest, I find that it's the employees own fault since they clearly didn't think before posting.

The employee had a concern about the practices of the company and there is nothing wrong with stating that, freedom of speech, its a right

---

I feel that social media activity and comments should not be monitored by an employer, under any circumstance.

There are consequences to actions. This employee's post could have potentially damaged this company's reputation and caused patron's/customers to become upset by portraying the company in a negative light. This company is owned by someone who depends on it for their livelihood and can't have employees damaging how the company is perceived. This employee should have thought about her irresponsibility before she posted this. The employer is absolutely justified by monitoring and taking action when his monitors show actions such as this.

I feel that whatever I post is a reflection of where I work and it's just disrespectful to post something like that.

Honestly, it was just my first reaction.

I think a further explanation from the employee would be warranted. There could be other individuals which results in a collectively small group who is responsible and management may not be aware of the poor decision and or actions of their employees. I think the firing of the employee is a little harsh and extreme. Another form of reprimanding should be utilized such as an employee suspension or demotion until a further investigation is completed.
I think that it was a bit overblown. But recycling is important

---

The person that posted questionable things should have been monitored by somebody for the sake of the brand itself. Companies can not allow regular worker to destroy the company`s image, brands are working too hard for that, for something like that to happen. So I am all for it. Monitoring is necessary.

I think that employers shouldn't check their employees social media. In my opinion it's unethical. Some people have a lot of information on social media that is sensitive, a lot of photos/posts that are intended only for their family/friends to see. Also, pictures and posts could be taken out of context, so they're not necessarily a reliable source of information.

---

i thought that was a good answer to the problem.

I don't believe any employer (minus like secret service agents, etc.) should be able to reprimand anyone for what they do on their own devices. I don't think they have the right to monitor what is done on personal devices. I do think if said person posted it via a company phone, computer, tablet, etc, the company would have rights to terminate said employee, but since it was done on a personal device, I completely disagree.

What if Corie's Facebook account was hacked and someone posted something about Taste of Beans Co. without him knowing. The employer is going too far with monitoring employees' social media activity, this would affect everyone's' privacy.

I just figure that is how I would react.

Because you should not post bad things about your work on social media. If you do then you should get fired because you are dishonoring the company.

Although I do kind of feel bad for Corie, I think they should have known better than to post something so negative about their company on social media. It's common sense, that that could have come back to bite them and cause problems for the company. Everyone should know that what they post on social media can be seen by everyone.

---

i thought it was ok because this is public information its out there for anyone to see
I think that it is justified that Justin's boss does monitor their social media use especially posts about the workplace because if your hired somewhere you should be positively representing the company everywhere. I think that he shouldn't of been fired though. I think the phone should have been confiscated and he should be put on probation.

It is not the companies duty to monitor what the workers think of policy on social media. The process seems like a big waste of time and the firing seems like a cover up to hid mismanagement.

The individual was using work-issued property, acting as an employee of the company, to make statements on behalf of the company. As such, the firm was well within its rights to control the actions of its employees with respect to use of company property and representations of the company.

I think that the employee has a reasonable expectation of privacy while using Facebook (assuming their profile was set to private, which I did assume because it was a coworker that showed the post to the boss). If the boss was not a Facebook friend and not the intended reader, then I think it violates the privacy of the sender. Also, I think the coworker that showed the messege to the boss is morally questionable and certainly a poor friend.
because of the behaviour of the people

When you agree to work for a company, you also agree to be a representative of that company. His actions directly and negatively described the company and its practices. I don't believe he should have been fired, though. A conversation and written warning should have been sufficient for a first offense. Companies have the right to monitor how those working for them are portraying their company and brand to the public. Corie didn't need to use the hashtag to bring the post to the company's attention. Additionally, this post was made while on company time.
By paying its employees to do a service, the company has the right to terminate someone who may be counter-productive to the task they have been hired to do.

I think if an employee is dumb enough to have a facebook that should be enough to get them fired alone. Then, if they are dumb enough to actually post something negative about the job on that facebook, then they definitely deserve to get fired for being an all around idiot and moron.
Because an employee shouldn't be tweeting at work first of all. They definitely shouldn't be saying bad things about their employer.

I am not sure how to think about this. It has never happened to me. If the company is misbehaving, there needs to be a way for a whistle blower to make the information known. But this seems kind of different. I am just not sure. Sorry!

Because I do not believe it is the employer's business. Perhaps, if it had come to light somehow, a discussion would be in order. As an employer, I'd be wary of this employee.

I feel like Facebook post are people's private lives and shouldn't reflect anything to do with work unless it's at the establishment, anything that happens outside of work or work hours is private.

if the employee violated some kind of signed agreement about not badmouthing the company, she totally merits getting fired. but perhaps less strict punishment if it wasn't a broken rule, just a really stupid move by the employee.

It isn't justified because what a person does and says beyond the workplace shouldn't be mandated by the company. And while I understand that badmouthing the company is bad for its image, perhaps a little introspection would be the better option. That is to say, perhaps the company should start working on how it handles its garbage instead of playing big brother to its employees. I don't think the employee should have said something, but forcing them to lose their job over it is an extreme reaction that only paints the company in an even more negative light, in my opinion.

---

i think the employee did a good think in the perspective of general public
I do not think that employees should be monitored, however when a post like that is brought to the employer's attention I understand the decision to fire the employee.

She should not be terminated for posting negative information about the company. By firing her, the company damages its credibility, gives the appearance of abuse of power by stifling dissent, and harms its social image. If what she said about the company was untrue, then they should ask her to correct her post or take legal action against her.Also, its seems invasive and scary that a company would monitor what is posted on their employees' personal social media accounts.
Corie had a good point observing that the company does not recycle even though it plays the responsible company. However, she should have let the managers know first and had it discussed. Monitoring the employees social media should not be the employers business.
While I don't disagree with the content of the post, it is completely fair for a company to require that employees not post about the company they work for, either in a positive or negative manner. The information can be inaccurate, misconstrued, or deliberately malicious. One should maintain separate or private accounts if they want to feel more freedom to post about their employers.

Social Media is that social media. It is in the public view so anything that is posted is fair game. Individuals should relize this when posting information. They put information out into a public view weather some one monitors it or not the boss still may have seen the picture. Now should she have been fired. No he could have repermanded her and asked to refrain from posting negative pictures of her place of employment and if refuses she could be asked to leave if she is so disatisifed with her employer.

I don't think that what the worker did was right. Why would she say something like that if she wanted to keep her job?

Employers should mind their business and quit snooping into people's personal lives. On the flip side, online isn't personal and people shouldn't post stupid things online that would get them in trouble.

People have no privacy anymore because of things like this. It's not acceptable to monitor what an employee does outside of work.

It's just how I felt in he moment.

because you should never denigrate your company on social media. you don't deserve to work there

Employees deserve the privacy of engaging in personal social behavior without that being breached by her line of work. If someone had saw her tweet and reported it to her workplace thats fine, but meticulously monitoring your employees to see if they say anything you disapprove of as an employer is unethical business practice.

I don't think it's ethic to post things about the place where you work.

You're using a company issued phone to post something negative about the company which is more than likely a violation of policy. Not smart and if you're going to post something so bold do it on your own device.

The phone was issued by the company and the post was not professional. I am sure the company shared their monitoring policy with their employee.

don't beleive companise have right to monitor employees behavior away from company
I believe this person is in the wrong and the manager has the right to do whatever they want with this person. It is a workplace. It is fair. It is just!!! We're all adults now.

If someone works for a company, it is common sense to talk about your company with respect in a public setting. The monitoring of social media was not the problem in this scenario, it was the choice the employee made to talk bad about the company on social media that got him fired.
It is not fair for personal life to have an affect on professional life. This is a personal social media account and the employee can say whatever they want.

My husband is a small business owner. They really have all the cards. They can do whatever they want to do.

An employee has responsibilities to his/her employer, and this includes not undermining the public perception of an organization or weakening the employer's brand with slanderous accusations. This tweet was a public statement that claimed the employer was hypocritical and should be viewed less well in the public eye relative to other companies. There was no fair analysis or comparison, merely a negative release of information and opinion of the company. Employers are not obligated to retain employees that intentionally undermine the company.

I feel like it is common practice to not mix social media and work. Most people that I know have a similar policy at their place of work. Before the "punchline" of telling the boss and getting fired, I had already assumed that would happen.

I feel it's in the best interest of a business to moniter the use of such things when it relates to it's brand.

Monitoring social media is a violation of privacy.

I went with what i feel make senes

Because he posted the issue on Social Media which was not smart at all.

It is not ethical to monitor or mix work with personal activities of their employees. Unless the employees signed a binding NDA about company practices, then the employee should not have been fired. Unreasonable termination due to invasion of privacy.

As an employee of a company, you should not disclose information that makes them look bad. Unless you're willing to be terminated.

---

good

IF IT WAS MY BUSINESS AND MY EMPLOYEE I WOULD HAVE FIRED HER. TO POST COMPANY INFORMATION ON SOCIAL MEDIA IS UNACCEPTABLE AND EVERY EMPLOYEE I HAVE I HAVE TOLD THIS VERY CLEARLY. TOTALLY UNACCEPTABLE AND THE FIRING WAS APPROPRIATE

In this situation I think that the employee had the right to their free speech. I would like to know if the statement is true through.

I would need more information to make a judgement, specifically, were employee told about the monitoring program and warned of potential consequences.

I think whatever personal feelings people have about their workplace should remain personal.

Most of the time companies lose out on business once an employee does something so wreck less.

It's a company issued phone.

Monitoring might increase quality but even might decrease it.

---

because the boss was doing a public search which means the person didn't have their settings set to private and its his own fault

---

It was a work issued phone, so it should be used for work only, so that was a punishable offense. It was unethical for her to post something offensive about the company she works for, especially on company time. Common sense would dictate that should she feel she needed to post this it should be done anonymously (thus not on Facebook), and not during work hours.

I think the employer had the right to check out someones social media during the hiring process but I dont think they have the right to snoop on your social media accounts just to be doing it.
I feel that they should check their social media to examine if they are behaving in ethical ways. However posts that prove dishonesty within the company should not be punishable.

Her comments could affect the look of the company but I'm not sure if she should be fired or not because I wasn't made aware of the company's policy of social media use by employees.
Unless the employee KNEW their social media was being monitored, it feels like a gross invasion of their privacy. Also, the company WAS handling their recycling the wrong way. However, perhaps the employee should have confronted management about this instead of posting on social media.

Under no circumstances should an employee portray the company they work for negatively on social media.

Businesses should not monitor employees personal communication.

I think that it is fair for the employee to monitor this activity because Corie was using a work issued phone. It should be common sense that this could be tracked. Furthermore, if the employee is trying to hurt their own company, that is an issue in and of itself.

I reacted this way because I did not feel there was anything was wrong with the monitoring process considering the situation.

It's terrible for someone to disparage the company that is giving them a salary. She was wrong to post something like that.

The company was doing something illegal, but the employee went about reporting it the wrong way.

EMPLOYEES ARE A REPRESENTATIVE OF THEIR EMPLOYER. THEY ARE THE IMAGE OF THE COMPANY AN DSHOULD SUPPORT THEM WHILE EMPLOYED

It is not good to post something like that on social media. Employees should always protect their costumer and their company

---

It was public information and if the employee didn't want it to be seen they shouldn't have published it. It's not a case for dismissal though.

I believe that the firing was justified because Corie should not have posted that on social media if she had any common sense and wanted to keep her job. It makes her look completely not trustworthy to her employer. If she was posting that then what else would she do.

In a country with freedom of speech, it is unjust for the employer to react to something the employee posts on their personal account. It's no different than if she told her friends that, the only difference is the audience may be larger. It is a violation of the employee's first amendment rights.

Employees' social media posts about their place of employment reflects on that place of employment. Managers have ever right to protect the business' reputation and image. That goes double since this was done on a work-issued cell phone.

The employee was not on the clock and was telling no lies. Unless he signed a nondisclosure agreement the employer was in the wrong.

The company has a right to see what the employee is posting online about the company. They should not fire them though. I think a suspension of some kind would be fine.
She posted it on social media with a hash tag for the business. Doing that made it public, where anyone could see it. The business did not violate the employee's privacy in any way. If you plan on being employed by a company, you can't bash the company over social media and expect to still have a job there.

The employee was using a company-issued phone and so had no expectation of privacy. Additionally, I am assuming that the employment agreement or company guidelines the employee agreed to upon accepting the job outline acceptable behavior, use of company equipment, and so forth. If the employee accepted these terms, the employer's actions are defensible (I might have given him a warning the first time, however). On the other hand, if the company has no pertinent policies that employees accept as a condition of employment, my opinion would be completely different and I would say the company is way out of bounds.
It's ok to disagree with workplace practices, but to do so on company time and social media is wrong. I do wonder if the company has a policy on social media usage?

I've been caught the same way after slamming my CEO for a big layoff. I felt good about it and the HR lady agreed so I kept my job. Of course in a couple weeks I quit that hell hole. Bottom line if you work for a place that monitors you like that, then quit and get a new job. We are not slaves!

Social media is basically the public these days by her posting that its like she's publicly bashing her company. I'm not sure if I feel she should be fired but I'm also not a manager/boss type personality .

I think that people should be able to post whatever they want to social media however, when it is done using a company-issued smartphone, it is the wrong thing to do. If she were to post that on her regular phone, I would have an issue with her being terminated. However, that phone is company property and shouldn't be used to access social media, etc. My husband uses his work phone only for work things. She should be able to do the same without getting on social media.
While I feel that the social media pages of employees are their personal property and they have the right to free speech, I also think that if you are going to publicly bash the company you work for then you should not work there. So firing her on the basis of this post is justified, but I don't think that employers should be able to monitor facebook posts. I was fired for something once for posting something entirely non work related, and it was extremely unfair.

The employee is acting as whistleblower. If the company claims that it recycles some of the trash it produces, and that claim is a lie, the customers have the right to know, as it may affect their decision to shop at that store.

I think a persons private life should remain private. Also, if what the employee said is true, it should not be used against him. If he was actually caught at work spending time on social media while he is suppose to be working, that is a different story.

This employee used a company issued cell phone to post the derogatory remark about the company. I feel the company has every right to monitor any texts, e-mail and social media postings made with their own phones. Because of the potentially damaging impact of the posting, firing the employee is reasonable because it is apparent the employee does not have the best interests of the company in mind.

I do not feel like we should terminate anyone working so hard but benefiting so much from the experience and labor they receive.

It wasn't clear if the employees were aware they were being monitored. If they were aware, and did this anyway, they are dumb and deserved it. If they had no idea, they expected privacy and didn't really deserve it.

People should be responsible with their social media posting. If they bad mouth their own company publicly, whether it's through speaking or online posting, they should accept the consequences of their bosses discovering it.

She was posting something honest about the company's practices that may concern customers. I can see how the post would be considered unprofessional and she should have gone about handling her complaint in a more serious way (e.g., not on social

media), however, customers have a right to know if the company is not staying true to its standards.

I personally feel like someones social life is none of the managers business.

This is a tough one. Im not too sure what I would do in the situation. I would probably fire an employee if there social media was open for anyone to see.

I think how people act outside of their jobs is up to them and so most people are different in their social media platforms as opposed to their professional settings, hence it is unfair to monitor and use their social medias to judge them or take action against them during work, Moreover, its unfair to take to an account how someone is outside of work being in their social media to judge their work ethics. I also disagree with the firing as I believe that the employee should've been given a second chance and told not to talk about the company outside of work, especially in a bad manner.

While I don't like the practice of the company monitoring their employees, the employee should not have posted about the company on social media, especially while on shift.

I think I can understand the necessity of a business to think they need to monitor their online business reputation, especially if an employee whom they are responsible for shares something negative online. On the other hand, the employee also has some rights, and perhaps the termination of the employee was too harsh and there could have been a different means of resolution.

I feel as though it is justifiable to monitor an employees social media presence, because by employing said person the company is then allowing the employee to publicly represent them and vise versa. I do not feel making a post about the recycling habits of a company would warrant the termination of an employee, especially if the company is claiming to be environmentally responsible while not acting that way. Disciplinary action could be justified. At the very least there is a greater problem at hand than recycling if an employee is bad mouthing an employer in a public forum, and I think it would be most beneficial to the company to find the root of the problem, instead of bandaging a symptom.

Overall, I am rather conflicted on the topic of cybervetting. Part of me believes that employees should be fully responsible for what is posted and shared to their social media account. Another part of me is kinda turned off by the fact that you have your manager going out of his way to look up your profile. (not in this case, but speaking in general)

I don't think Corie should have posted that. It's not nice, but it IS true. Does he have something in his contract that states he can't post? If not, if there is no rule, then the firing is bogus. I don't think jobs should spy on people's private lives, but it is the internet and when people put things out there, it's free game.

I believe an employer has the right to monitor social media posts made by employees. That being said, I also believe that the employee should be given fair warning. So, in the scenario, it's questionable as to whether or not Corie should have been fired. If she knew she was being monitored and if she knew saying derogatory things about the company was a valid reason for being let go, then, yes, it was a fair consequence.

I react to the monitoring practice questions. But I do feel the company is justified in the firing due to what the employee posted about the place he works at.

I think we should have more privacy in social networks

I believe that the employee was entitled to freedom of speech on her own private social media. I do believe that what the employee said was inappropriate but this was an opportunity to make the company better by listening to the opinions of employees.

I believe that one should be able to express one's opinion in their own social outlet however they which. If he was sending that message on the company official account that would be another matter.

I think for the most part it is a bad practice to monitor employees' personal lives as long as it doesn't affect their work performance. I think that while the employer may have had justification for the firing since it was through a work issued phone, but beyond that, it mostly seems like the boss was just mad that the employee made his extremely deceptive and unethical business practices public. I think there is far more justification for the boss to lose his job for lying about recycling than an employee blowing the whistle on him.

The employee has right to their opinion but if they are bad mouthing their employee during working hours well I would have firedx him too. YI feel you should be loyal to your company and if you are not why would you work for them anyhow. I feel bad that employers can not trust everyone they hire but I feel they should monitor and eventually they will see who is worth keeping and who is not. Why would you want to give your business a bad name espciallyl if you want to keep working there. Just awful

---

In this case, they did not have to invade Corie's privacy by using her personal information (i.e. social media login info). Corie posted something on her social media and allowed it to be viewed by other people on her own free will.

I don't think it is the employer's place to monitor personal social media accounts. If it was an account or application that was on the employer's network, then it would be different. However, I do agree that the employee should be penalized for using the employer's name in a hashtag. I don't think firing is appropriate unless a policy was in place that explicitly stated that was the consequences of posting negative information.

Because the boss invaded her privacy. What you say outside your work place or that involves a personal item....i.e Smartphone, is an intrusion of privacy. What's next?

Monitoring your family and friends on your personal needs? Will politicians intrude on the lives of their constituents and see who is for or against them? It sets a pattern.

---

i felt that the boss as the right to monitor his/her employees to the fullest. He has t business to run and needs to know what his employees are up to and if the job is getting done. I felt that the employee was justified in getting fired because of what I just explained.

What employees do when not on the clock is none of the company's business. I realize that the Corie was at work when she posted on social media and that, she should be coached for. Not fired. Perhaps the company should be sure that what she posted isn't true.

I believe that if you put information out there for anyone to see, including your employer, you should be prepared to be held responsible for any negative repercussions that can come from it.
It's not right to get fired because of some Facebook if it's a good worker and it's also not right for a worker to use a phone for Facebook during working hour.

Social media is a form of expression alongside writing and speech. If an employee were standing behind the counter trash-talking the company, they would be written up or fired, so it makes sense that the same rules apply to social media. However, if this hadn't happened on the clock then I would be much less supportive of it; what an employee does after hours is their business, not the company's.

I think it's more important for businesses to be transparent about their practices. Although the employee acted "unprofessionally" by posting it, the business is more in the wrong for the lack of transparency about their recycling. It's deceptive to provide recycling containers to customers who, by putting recyclables in the container, are very intentional about their desire to recycle, and then promptly negating their efforts by throwing it out with the rest of the trash. On top of this, firing an employee for rightly calling it out is even more shady. In general it seems very invasive to monitor your employees' activity online, but I can see why it may be justified to fire an employee if their online activity harms customers in any way. This does not appear to be that kind of case.

Once the employee posted something on social media, she made her thoughts public. This is comparable to sharing her thoughts verbally with someone while she's on break. This is not acceptable. If the scenario had been that she shared this remark in a private email outside of work hours, that would be completely different. However, putting it on a public forum makes it accessible to everyone and her boss had every right to fire her.

Because you are supposed to monitor your employees if that's your job
I don't know if it's "fair" or not, because I don't know if the employee is allowed to engage in social media using his work-issued device, whether they know they're being monitored, and if they are aware of the consequences.

I think that when an employer monitors your social media it is an invasion of privacy, however, when you hashtag the company and let the world see something like that, then being fired for publicly trashing the company's name is completely acceptable.

You didn't say if the company told employees they would be monitored, and if this was legal, or if they could be fired for their posts. If the employee had been told, he surely could be fired. If not, maybe he shouldn't be fired or disciplined. If the monitoring was illegal, he shouldn't be disciplined.

---

because i believe the monitor process is fair to the consumer

---

He should not be posting on social media anything negative about his employer. The owner wants to know what his employees are doing in his work place, and probably already made that clear at sometime during the employee's hiring.

I think it is fair that a company protect its reputation and brand image, as that is a major factor in successful businesses. I do think the employee should have been given at least one chance before being fired, if this was her only and first infraction. She should have been asked to delete the post and refrain from posting again, or she would be fired at that point.

---

because I agree that the managers monitor the social networks of employees in this way you can realize the heads of loyalty of people who work for the company, the comment posted by this person is very degrading .... now that deserves or not what happened to him after they gave him the number he had posted that then, if I do not know if he is right or wrong, what happened to him

---

She divulged sensitive company information in a very negative way.

I feel there should be regulations regarding employers rights to invade an individual's privacy. The employer's screening and hiring practices should be sufficient to determine hiring without snooping on facebook. On the other hand, I feel that people who are stupid enough to post anti-employer information should not be surprised when they find themselves in the unemployment line.

Employees are expected to be the face of the brand. Corie was sending out this message during work time, on her work device --- She was representing the company.

Employee's need to positively represent the company they work for and this is a misuse of company property.

Some companies try and empower employees as much as they can. At the same time, there can be problems when employees sort of cross into that undefined space where they are critical of a company without actually providing a solution- something I believe that

should be trained in and rewarded. Having those systems in place, it isn't possible that a company can ignore what people are saying about it in public venues. A popular facebook poster may have thousands of people in the local community watching what they do on social media. It is therefore pretty appropriate for a company that wants to maintain its image to rely upon news about themselves by listening to external and internal feedback people.

I dont think its right to spy on employees like that.

Workers are entitled to opinions. It's healthy to vent or we will all go crazy. There should be freedom of speech, besides no one cares what one employees posts and one could argue that it may or may not be true..but If it is true all the more reason for him to be allowed to express a thought.

I feel like it is wrong for companies to monitor social media, but that being said, if you do something stupid on social media and your company finds out, it's kind of your own fault if you get in trouble or fired!

I think that employers should monitor their employees social media but I don't think she should have been fired for that statement especially if it was a true practice. I think she has a law suit on her hands.

I guess the employer has a right to monitor use of their equipment, but they should be recycling as well.

I feel that a person has the right to privacy. If an employee is on their break, That is not the same as being on the company's time. Plus he Corie was using his own smartphone, Not a computer belonging to the Taste of Beans co.

If the employee knew that was a policy that the Employer was going to uphold, then with the remark that was made about the company, to me seems like grounds for termination.

In today's world, you have to be aware that you can be held accountable for anything you post online, and usually the things you least want seen are the ones people notice the most.

Tp fire someone just because of their opinion seems kind of silly to me. I can understand the boss being upset but the employee didn't really do anything that was that bad and at the end of the day it doesn't really hurt the companies reputation in the grand scheme of things.

No disrespecting a company but i feel they should recycle. The employee should of not posted information or tell a friend.

I think this employee should not posting negative comments about the company' environmental policy using Social Media, without the approval of the corporation. However, the employee has 1st amendment rights and those should remain protected against lawsuits from the company after she is terminated.

I think the monitoring of social media by an employer is justified to a point. If the employee is posting a lot of negative things about the business then it is justified the employee should get fired. I don't think monitoring ALL of the social media posts is justified. There could be sensitive, personal things that an employee wouldn't want the employer to see.

I don't feel that the company was monitoring the employee. the employee was a facebook friend with another employee who saw the post and reported it. the post by the employee is slander against the employer and can be reposted and reposted causing harm to the company. I am sure that there is a violation in ethics because she posted a photo of the work environment and slandered her employer.

Because it said it was a work issued cell phone so in my opinion they have the right to monitor it if they pay for it. If it was his personal phone it may have been different but I think the decision to fire him was justified also

---

It can be justified to monitor in this case because even though Corie posted to Facebook during his short off-duty break and maybe used his personal account, but he did it by using work-issued smartphone. He should have done it using his private phone.

I'm unsure how I would react and I do not drink coffee or work in the service industry!

Whatever happened to privacy and rights of speech? If posting something on sociail media was against the rules then there should be a protical ie; warning (written) then termination.

Employers should be able to monitor employees social media usage as it pertains to the business. If an employee is bad mouthing the business then they should not be working there.

People have a right to have a life outside of work. The employee was saying something that might be bad PR for the company, but the employer had to right to monitor the employee's social media unless informed by someone. It was like the employee was guilty until proven innocent when it should be the opposite.

As an employee of a company on company time one is expected to represent the company well. To post negative comments about the hand that feeds you so to speak is just not acceptable. There are other ways to deal with opinions about what an employer is not doing correctly. Once it is on social media everyone should know it is public and viewable by everyone even if they are not directly allowed access to the account.

Because employees have a right to voice their opinions to their friends on their social media without being monitored.

It was an employer issued phone that she used to post, and it was also a very negative post against her employer in that post.

It was a work phone. He should not be posting such things with a work phone

The employee was using a company-issued phone to put the post on Facebook, so the company has a right to see how the phone was used. The employee made negative comments about the company she was working for in a public forum, so is held accountable for what she says.

His boss wasn't "monitoring" him. he CHOSE to be friends with a snitch of a coworker on Facebook and that's his own goddamn fault.

It's unethical and immoral.Firing an employee would not make people trust brand again, rather it would upset customers more! Company should focus more on making sure issue mentioned in the post is addressed instead.

It's not ok to publicly post private company information. Even worse, the post tagged the company on its public website.

I think that sometimes employees should be monitored due to professionalism. I think employees need to realize that companies are making sure that their businesses are trying to keep their images. But people do have the right to speech their mind but their are consquences
It is important to maintain professional behavior. Her comments were inappropriate, and there was likely a better way to handle her concerns.

I believe you should watch what you say even on social media. You definitely shouldn't talk down about your job on social media.

The employee is making comments about the company she works for. It's very damaging to her employer for comments like that to be made. If she has an issue with the company, she should bring it up internally to address it. Not through a social media post.

I don't feel like it was a fireable offense. A counseling would have sufficed
I think it would be good to monitor employees.

Since it was the employee's personal social media account, it did not seem appropriate for her employer to be monitoring that account. Since the employee had tagged the company in the post anyway, the employer's social media team would have been better off

acknowledging the company's mistake, and bringing it to management's attention to correct the recycling error.

I think it was fair for the employer to monitor the employees post, since he posted it to social media, for the entire world to see. He even hash tagged the company's name and made no effort to make his post anonymous, so I get the impression that he didn't care who saw the post. Yet, he shouldn't have gotten fired for posting his opinion. It should have opened up a dialogue between him and the company to discuss his concerns and for them to mediate the situation. It is not fair to fire someone just because they voice their own opinion that may be different from what the company believes. They used their position of authority over him, and probably used him as an example to put fear in their other employees to all be "yes-people" or face the same consequences.

I reacted this way, because I believe the company should be able to monitor the social media activity of employees. I believe an employer should be able to fire an employee if they post something that could damage the companies reputation or brand, such as the employee posting in social media about the company not recycling. The employee in this case wrote that they believe the customers "would flip" if they knew the company threw recyclables in the dumpster. They posted this, with the knowledge that it could hurt the company.

Social media should never be used in these situations. Someone's work should always be separated from their social media. One must understand that before posting or doing anything on their accounts.

The employer does have a right to protect it's image. Employee should not have posted with their employer's name.

---

that is private information expressing his opinions outside of company cant fire people that the situation has nothin to do with his ability to do his job

---

When you post something publicly, anyone has the right to look at it. If I had an employee bad mouthing my business I wouldn't want them working for me either.

I'm torn on this one. I do think the boss fired the employee in haste. If there had been other infractions committed by the employee, then yes, the termination was justified. On the flip side...social media is just that "social" media, meaning everyone has access to it. If you don't want your comments or actions to be reviewed by everyone and possibly affect your life, don't post them.

Although I feel for the person that got fired on posting on what they thought was tehir personal account they can share freely with, they must realize that what they put on the internet, ESPECIALLY if it was negative toward the company that employs her, is fair game and can be used against her. Businesses obssess over reviews on the internet, so

why wouldn't they be concerned over their own employee negatively tarnishing their name and reputation?
The employee put something on social media that could cause the business to lose customers
The company should outline their social media policy and requirements for termination.
Employers have a right to excuse employees who deliberately undermined the company.
The employee should have discussed this with her employer to resolve the issue.

I think if an employee is using social media while on the clock, that is a fire-able offense in addition to posting internal company details or disparaging the employer on social media.
Corie knew the cell phone was monitored. I'm sure he was supposed to be doing work related things on there. I think it was freedom of speech But he should have known he would get fired for doing that.

I think it's important to support the company you work for and not talk negatively in social media about your company. Also, what you post on social media is a reflection of you, which in turn is a reflection on your company.

The employee who posted to facebook posted negatively on the company, potentially giving them a bad reputation. In addition, the company could lose profits. And the person used vulgar language, emphasizing a possible level of discontentment of being employed there. A better way to handle the situation might have been to raise the concern to the supervisor, so as to promote change in a positive way rather than just expressing frustration and slandering the company in real time. It also might have given this employee some future opportunities by being seen as someone who tries to make things better and come up with solutions.

Because I don't think an employee should bad mouth the company they work for unless they are prepared to quit or be fired.

As an employee of Taste of Beans, Corie had an obligation to represent the company in a respectful and positive way. If I was paying someone to represent me or my brand, I would want to make sure they were not posting anything negative or anything that would hurt my business.
I think it is the responsibility of an employee to be respectful of the company they work for and not let their personal feelings interrupt the business they work for. Also employer's have the right to hold employee's accountable for their actions.

Because its too invasive

Its tough, because she was talking about work. But it was on her personal time. I just dont agree with jobs and corporations controlling our personal lives and opinions for their profit.

The employee should not have posted what he did but his employer could have disciplined him in some way other than firing him.

I reacted this way because he was talking badly about the company. It's up to the company to protect themselves and his post put them in a negative light. While he may be telling the truth it's not okay to post that kind of thing on social media.

In this particular scenario I think speaking with the employee about it if you notice it is reasonable. The employee was sharing valid information (assuming it was true) which is not about trade secrets or practices, and the only reason the company wouldn't want that is they look bad for not recycling as they claim. I don't think it's reasonable to fire someone for telling a truth like that. However, the employee did hastag the company which is a not a reasonable move and simply will cause the managers and owners added stress beyond just expressing herself, and I think she would need to understand that. Employees should be free to post any factual information that is not secretive for good reason, but they should do so in a way that is separate from the company itself, like not committing a crime in your work uniform.

I reacted this way, because I feel that when you are an employee of a business, you need to take that into consideration when you are posting on social media... I don't care if it's your personal page or not. You have to be respectful, especially when talking about work or something that happens at work.

She is representing a company and if she had an issue with the way they do things, she should have spoke to management or HR. I think that social media activity when representing a company should be looked at, especially since she tagged the company.

It is something that they shouldnt be monitoring

---

because this person was a whistle blower and more than likely be protected under this law

---

Based on this example, the employee used a company issues device on company time. I think it's fine for the boss to monitor company property and time. Also, I believe it was a misuse of the device and could hurt the business so I think firing the employee was justifiable.

The employee had a right to share that information if the company was telling lies to consumers about its sustainable practices. The company should have asked the employee to discuss such things with them first in the future not fire them. Just seems like the company were intentionally trying to hide the information if they fired Corie.

The info posted is disparaging to the company, but I think during for a first offense may be too harsh. Perhaps a warning then firing. Corie, no doubt, signed a company policy on social media, do she should know what she did was not allowed. She also used corporate

property to post. Although I don't agree with employers monitoring employees social media accounts, in the case of using corporate property to do so, while on the clock (breaks are generally paid time) I agree that monitoring is okay.

Any information about the internal affairs of the company must be kept confidential. It does not matter whether it's bad or good. In addition, if an employee has time to publish posts, then he does not work well.

As Americans we have a right to voice our opinions and while Corie was on the clock and Facebook and that is not cool he did nothing else wrong that deserved him being fired. For all we know he could have been on his break when he posted this and not on company time. It is whistle blowers like Corie that help protect our land and others. It is wrong of the company to claim to be economically responsible and not recycle. I am sure there are customers that chose to frequent this company to help reduce their own footprint on the world and they would be livid knowing the company is not holding up there claims. I would be!

I don't think an employee should disrespect the company in which they are employed.

Although an employee has the option to limit those who can see his/her posts, in this particular scenario I consider the termination to be very similar to firing a whistleblower. First of all, the employer was not the one who found the Facebook post, so it's unknown if the employer does any monitoring. I think it's acceptable to monitor employee social media use on company time. And a smart company will look for any mention of it on social media whether by an employee or not. This can allow them to respond to any customer concerns. In this case I think the firing was uncalled for if the allegation was true.

If the employee was informed that the boss would be monitoring their social media, they shouldn't have written such a stupid post. I think the boss was right in firing the employee for a potentially damaging message.

I feel like he should know the phone is a phone being provided by the company so whatever he chooses to do or say can and will be monitored so i feel him saying negative things about the company is absolutely justified.

I think that Corie being fired for that is appropriate, because as an employee of a company you're representing your company at all times, and I wouldn't anyone I work with to say negative things about the company we work for online. The reason I was indecisive about if monitoring is okay or not just depends on the way the employer goes about it. Employees should definitely be told they'll be monitored, it should never be in secret.

---

they were angry that the employee was giving him a bad name

Should not have posted that type of comment on social media.

You should never comment about your job on social media or about it at all.What goes on at work should never be discussed on or off social media.

The employer has a right to not have employees disparage the company. The employee is ignorant enough not to apply some security to their social media so every inane thing they post isn't blasted to the public. The employee gave no verifiable proof of a disparaging remark. This could mean a loss of business (from people who don't bother to verify internet 'facts') and this could be a legal offense.

Firing an employee can have a catastrophic, long-term impact on the employee’s life vastly out of proportion to the offense.

I think the lack of awareness of the employee is a signal that this is not the right place for them to be employed

---

If a person is working for a specific company, he shouldn't act opposite to that company.. This is my feeling..

I think it was crappy of Corie to post that, but the boss has no right to fire her for posting her opinion. Well, it's his company so yeah I guess he could fire her it was a dumb move. But there is freedom of speech (and to lose one's job). I think they both should have worked together to solve the issue.

The employer is worried about the employee exposing their practices. If the employer was being He used a COMPANY phone for one. Also #the company name on something negative about the company. I would fire them also

---

The employee chose to share negative remarks on a PUBLIC platform. If the employee was concerned about online privacy she should have shared her thoughts on a forum that was a bit more private.

As an employee of a company, you represent that company. Posting what she said which is negative is unacceptable as an employee. It is within the boss's right to monitor especially since she was on the clock when she posted that.

When you work for a company you represent that company. If you are going to go around bad mouthing that company to the world and tarnishing their image the company has the right to fire you. Seeing it on a post is no different than if they had seen it in the newspaper or on regular news. Nobody objects to that.

I think that's totally fair because that really hurts the company's image and there is no way for people to actually know if what that person posted is true or not. For example, they could have taken a photo of throwing recyclables in the dumpster and then just took

that photo to make the company look bad because they were angry about something else. It hurts the brand's image and part of being an employee of a chain is that you don't say negative things about the brand, especially not on social media where it can spread and go viral very quickly.
I didn't feel that the post was harmful or wrong. The worker exposed a practice that was questionable. I also don't like when companies monitor social media as they might use that to fire employees with radically progressive views or who are not the "right" orientation/gender-presentation/gender-identity/whatever-else (an issue close to my own heart as I am a lesbian).
When employees use social media to comment on their employers, that information becomes public. Employees can be held responsible for comments they make that they choose to share publicly.

I don't recall if there is a social media policy in effect that the employee signed and if she was aware of the monitoring. So I'm conflicted because if she knew she'd be fired then it's fair. However if there was no policy than I side with her. I don’t think people in most positions should be fired for social media posts. I also don’t like the monitoring but if it’s in the company’s policy...

I think it's common practice.

It was a work-issued device, and it was used to post the message while at work. It is one thing to do it on your own time, with your own technology, and something else to do it as she did in this situation. Hopefully the employees were briefed on this when they started with their employment. Plus, I wouldn't think it was something that she should be fireable for on her first offense. If she was otherwise a model employee then a warning would suffice. If she was a problematic employee, however, then it was justified.

A company has no business monitoring an employee's social media activity, any more than it has a right to monitor their activities after they leave work for the day. Do employees go to a certain bar after work, or play softball together, or just go home to their families and watch television? In any case, it is no business of the company what they do. On the other hand, the employee involved in this situation was, according to the scenario, on company time when she sent her post -- she was not on a lunch break or anything. On the other hand, she was using her own smartphone, not one of the company's computers. So, this is a slightly complicated situation but after all is said and done I would definitely come down on the side of the employee in this case. Butt out, Big Brother!

In my opinion I believe the employee of any company should be able to give their honest opinions about the company in which they work at

---

I don't necessarily think that it is fair to the employee, however, if it is a known condition of employment, than so be it. I understand the employer wanting/needing to do this. Bottom line, don't bite the hand that feeds you.

An employee has a certain basic responsibility to the employer. Freedom of speech does not apply to badmouthing your employee.

While the company has a right to run its business as it deems necessary and to be interested in employee's loyalties to their employer, the company's ethics were fodder for discussion. I just think that Corie ought to have taken her concerns to the business owner instead of social media. It is possible that the manager was allowing questionable protocol that the business owner would've disapproved of.

It was inappropriate for her to post a negative evaluation of her employer. Her employer has every right to look at her social media posts. Posting on social media is done at a person's own risk. I don't blame the employer for firing someone who is causing the public to see his company poorly.

I really don't think the employee should've been fired. May tell them if they ever did anything like that again they would be but not fire them

---

I am kind of tased on this issue. Because a Facebook account should be your personal business. But if you are bad mouthing your company or putting out their secrets then yes you should be held accountable for that.

That post was obviously vindictive towards the company, so I feel like the manager had an absolute right to terminate their employment.

Because Corie posted it during his shift by using his private cell phone which is unethical to do.
It is important that employees maintain the dignity of the place the work for. If they cannot, then they should not work there. Given everything people do on social media, it is in an employer’s best interest to monitor employees.

APPENDIX K: IRB APPROVAL

IRB
INSTITUTIONAL REVIEW BOARD
Office of Research Compliance,
010A Sam Ingram Building,
2269 Middle Tennessee Blvd
Murfreesboro, TN 37129

MIDDLE TENNESSEE STATE UNIVERSITY

IRBN007 – EXEMPTION DETERMINATION NOTICE

Thursday, March 15, 2018

Investigator(s): Melissa McCord; Judith van Hein
Investigator(s') Email(s): mnm4e@mtmail.mtsu.edu; judy.vanhein@mtsu.edu
Department: Psychology

Study Title: Employees' fairness perceptions of workplace social media monitoring: Privacy invasiveness, smartphone ownership, and work periods
Protocol ID: **18-1171**

Dear Investigator(s),

The above identified research proposal has been reviewed by the MTSU Institutional Review Board (IRB) through the **EXEMPT** review mechanism under 45 CFR 46.101(b)(2) within the research category *(2) Educational Tests* A summary of the IRB action and other particulars in regard to this protocol application is tabulated as shown below:

IRB Action	EXEMPT from further IRB review***	
Date of expiration	NOT APPLICABLE	
Participant Size	1000 [One Thousand]	
Participant Pool	Adults 18+	
Mandatory Restrictions	1. Participants must be age 18+ 2 Informed consent must be obtained 3. Identifiable information may not be collected/stored with participant respoinses	
Additional Restrictions	None at this time	
Comments	None at this time	
Amendments	Date	Post-Approval Amendments NONE

***This exemption determination only allows above defined protocol from further IRB review such as continuing review. However, the following post-approval requirements still apply:

- Addition/removal of subject population should not be implemented without IRB approval
- Change in investigators must be notified and approved
- Modifications to procedures must be clearly articulated in an addendum request and the proposed changes must not be incorporated without an approval
- Be advised that the proposed change must comply within the requirements for exemption
- Changes to the research location must be approved – appropriate permission letter(s) from external institutions must accompany the addendum request form

- Changes to funding source must be notified via email (irb_submissions@mtsu.edu)
- The exemption does not expire as long as the protocol is in good standing
- Project completion must be reported via email (irb_submissions@mtsu.edu)
- Research-related injuries to the participants and other events must be reported within 48 hours of such events to compliance@mtsu.edu

The current MTSU IRB policies allow the investigators to make the following types of changes to this protocol without the need to report to the Office of Compliance, as long as the proposed changes do not result in the cancellation of the protocols eligibility for exemption:

- Editorial and minor administrative revisions to the consent form or other study documents
- Increasing/decreasing the participant size

The investigator(s) indicated in this notification should read and abide by all applicable post-approval conditions imposed with this approval. Refer to the post-approval guidelines posted in the MTSU IRB's website. Any unanticipated harms to participants or adverse events must be reported to the Office of Compliance at (615) 494-8918 within 48 hours of the incident.

All of the research-related records, which include signed consent forms, current & past investigator information, training certificates, survey instruments and other documents related to the study, must be retained by the PI or the faculty advisor (if the PI is a student) at the sacure location mentioned in the protocol application. The data storage must be maintained for at least three (3) years after study completion. Subsequently, the researcher may destroy the data in a manner that maintains confidentiality and anonymity. IRB reserves the right to modify, change or cancel the terms of this letter without prior notice. Be advised that IRB also reserves the right to inspect or audit your records if needed.

Sincerely,

Institutional Review Board
Middle Tennessee State University

Quick Links:

Click here for a detailed list of the post-approval responsibilities.
More information on exmpt procedures can be found here.