International Journal of Business & Law Research 4(3):37-57, July-Sept. 2016, 2016

© SEAHI PUBLICATIONS, 2016 **www.seahipaj.org** **ISSN: 2360-8986**

The Intentional Tort of Invasion of Privacy in the Private Employment Sector: Legal Analysis and Recommendations for Managers

Frank J. Cavico[1] & Bahaudin G. Mujtaba[2]

[1]Professor of Business Law and Ethics
The H. Wayne Huizenga College of Business and Entrepreneurship
Nova Southeastern University, Fort Lauderdale, USA
Email: cavico@nova.edu
Phone: 954 262-5096

[2]Professor of Management (Contact Person)
The H. Wayne Huizenga College of Business and Entrepreneurship
Nova Southeastern University, Fort Lauderdale, USA
Email: mujtaba@nova.edu
Phone: 954 262-5045

ABSTRACT
The modern workplace requires that employers have access to a great deal of information about their worker, customers and suppliers for legitimate reasons. As such, employers must protect their access to all this information in order to protect themselves from any legal liability. This article focuses on employment and privacy law by examining the common law intentional tort of invasion of privacy in the private sector workplace. While employers can have good reasons as well as the legal right to engage in monitoring, searching, and surveillance of their employees that legal latitude is not without bounds. "Reasonableness" is a key factor in this legal analysis as it is with much of tort law.
The authors stress that surveillance, searching, and monitoring policies must be not only legal, but also fair, dignified and respectful to the employees. In addition to avoiding legal liability acting in such a legal and ethical manner is in the long-term interest of the employer in attracting and maintaining high quality employees as well as to achieving and maintaining a good reputation with clients, customers, shareholders, the community, and the legal system. Suggestions and recommendations are provided for managers and employers.
Keywords: Tort, invasion of privacy, intentional torts.

INTRODUCTION

This article is an examination of the common law intentional tort of invasion of privacy in the private sector employment sector. Following this introductory section is a limitations section where the authors mention the limitations of this article, the main one being that this legal analysis focuses on the private sector and not the public sector. The article next discusses the rationales for employer to engage in the surveillance, searching, and monitoring of its employees. As will be seen, the employer having a legitimate reason for any perceived intrusion into privacy is a very important factor in determining

liability. The article then presents a detailed legal analysis of the tort. A legal overview is first offered; and then the authors discuss the general principles of the tort, the damages, defenses, and the intent factor. The authors next discuss the critical private sphere or private concern element to the tort where an employee may have a reasonable expectation of privacy. The authors then examine the means of the intrusion and its degree of offensiveness, which degree is another critical element to the tort. The place of any surveillance is also discussed as another factor impacting liability. Next, the authors again discuss possible legitimate reasons for the employer to engage in surveillance and other perceived intrusive conduct and provide examples therewith. The authors also provide an examination of employer electronic monitoring focusing on monitoring email. Next, in a separate part to the article the authors briefly discuss another aspect to the tort of invasion of privacy – the tort of public disclosure of private information – stating its key elements and providing examples. These preceding legal sections culminate in a brief legal conclusion. Following the preceding legal analysis the authors discuss the implications of this tort for managers; and then the authors supply several recommendations to management to avoid liability for the intentional tort of invasion of privacy. The article concludes with a brief summary and conclusion.

There are many circumstances where invasion of privacy issues could arise in the employment context. Green (2001, pp. 4-6) lists several, to wit:

- The employer secretly videotapes the employee in the workplace or off-the-job, perhaps to discover information that the employer feels would be detrimental to its business.
- The employer conducts a physical search of the employee, perhaps as part of an investigation as to a theft.
- The employer monitors the employees electronically, perhaps to "police" any perceived sexual harassment activity.
- The employer conducts surveillance of the employee's off-duty activities, perhaps to discover violations of an anti-nepotism or anti-dating policy or to see if the employee is making improper disclosures to competitors.
- The employer discloses without the employee's consent certain private information about the employee, for example that s/he is recently divorced or is diabetic or HIV positive.

Keller (2013, p. 986) adds the following additional examples of employer intrusions:

- Opening the employee's private personal mail.
- Searching an employee's safe or wallet.
- Examining an employee's private bank account.
- Tricking or deceiving an employee to allow an examination of his or her personal records.

The seminal issue herein is whether any or all of the preceding intrusions as well as others to be examined in this article rise to the level of the intentional tort of invasion of privacy. This article has several limitations which will be briefly mentioned in the next section and which certainly could be viewed as topics for future academic research and writing endeavors.

LIMITATIONS TO THIS ARTICLE

The subject matter of privacy, and even privacy in employment, is a vast area of the law encompassing the U.S. Constitution, state constitutions, federal and state statutes, administrative rules and regulations, as well as the common law (that is, judge-made case law). This article, as indicated by the title, takes a narrow "slice" of this large legal "pie" by focusing on the private employment sector and one legal wrong - the intentional tort of invasion of privacy. Tort law is civil law based on the common law which goes back to Old English Days. Constitutions, statutes, and agency rules will be mentioned but the focal point will be on the common law intentional tort of invasion of privacy. As such, since the examination will be mainly on the private employment sector, such issues pertaining to invasions in public sector, that is, by government employers, will not be covered, to wit: the Constitutional right to privacy as recognized by the U.S. Supreme Court and implied from the 1st, 3rd, 4th, 5th, and 9th amendments, the 4th Amendment prohibition against unreasonable search and seizure and the 14th Amendment Due Process protections for

"liberty" and "property" interests, and privacy rights pursuant to state constitutions (Cheeseman, 2014; Cavico and Mujtaba, 2014; Clarkson, Miller, Cross, 2012; Wesche, 2002; *Levi Wilson v. Scott Lamp, State of Iowa, Jessica Dorhout-Van Engen, and John Doe*, 2015; *O'Connor v. Ortega*, 1987; *Forsberg v. Housing Authority of Miami Beach*, 1984). Some public sector examples will be provided, however; and it also should be pointed out that the U.S. Supreme Court in a public sector employment context has said that the degree of privacy reasonably expected by public sector employees should be evaluated on a case-by-case basis (*O'Connor v. Ortega*, 1987, pp. 717-18). One will clearly see that this case-by-case approach will emerge in the private sector privacy context too. This article also will not address employment privacy disputes arising out of collective bargaining agreements pursuant to labor law or the National Labor Relations Act (NLRA), though whether employees "venting" about their employers on social media rises to the level of protected concerted activities protected by the NLRA is an important, most interesting, and rapidly developing, area of the law.

Moreover, the intentional tort of invasion of privacy, as will be seen, encompasses four separate, though naturally related, legal wrongs: intrusion into seclusion, public disclosure of private facts, appropriation of name or likeness, and false light disclosures (Cavico and Mujtaba, 2014; *Comprehensive Care Corporation v. Katzman*, 2010; *Jews for Jesus, Inc. v. Rapp*, 2008; Keeton, *et. al*., 1984). This article will discuss two aspects of the invasion of privacy tort: intrusion on seclusion and public disclosure of private facts, with prominent attention given to the former. Finally, invasions of privacy can be committed by both employers and employees; and, furthermore, the employer cannot only be directly liable for committing the tort but also may be vicariously liable (that is, the liability is imputed to the employer regardless of any employer culpability) pursuant to the doctrine of *respondeat superior* ("let the master answer for the wrongs of the servant") when an employee commits the tort during the course and scope of employment (*Courtney R. Robbins v. The Trustees of Indiana University and Clarian Health Partners, Inc.*, 2015; *Sharon Diane Waltz v. Jonathan Wade Dunning*, 2015; Cavico and Mujtaba, 2014; Keeton, *et. al*., 1984). Due to the management focus of this article as well as the constraints of time and space the authors will primarily examine the employer's direct liability in invading the privacy of its own employees and thereby committing the tort violation.

A final limitation of this article is the area of law usually called Lifestyle Protection Acts. These are state statutes, and many states have enacted such acts, that provide a degree of protection to employees who engage in *lawful* off-the-job activities and/or associations. These statutes provide protections against discharge to employees, even employees at-will (that is, those employees without any contractual limitations on their termination) whose activities fall within the purview of the statutes, for example, smoking tobacco products (Cavico and Mujtaba, 2014; Sprague, Spring, 2008). However, it is important to point out these statutes, though providing some privacy protection to employees, have exceptions benefitting the employer, for example, by stating that the employee can be discharged if the employees' activities or associations harm the employer from an economic and/or reputational standpoint or are a conflict-of-interest (Cavico and Mujtaba, 2014; Sprague, 2008). Of course, the employer must be careful in taking advantage of a statutory exception so as not to commit an impermissible invasion of privacy tort in determining if an exception applies. Since there are so many Lifestyle Protection Acts and they vary from state-to-state the authors will save that statutory comparative analysis for a future work. The next section to this article discusses employer rationales for the surveillance, searching, and monitoring of its employees, which as noted is an important feature in this area of the law.

EMPLOYER SURVEILLANCE, SEARCHING, AND MONITORING

An employer can have many reasons for conducting surveillance and monitoring of its employees – in the workplace and off-the-job – and by physical and electronic means. An employer may want to investigate performance issues, particularly the lack thereof, as well as to try to improve safety, performance, efficiency, and productivity (Mujtaba, 2014; Keller, 2013; Sprague, 2008; Nichols, 2001; Cavico, 1993). Management, supervision, and training are proper reasons for surveillance, searching, or monitoring, for example, of the employees' work-related phone calls (*Ali v. Douglas Cable Communications*, 1996),

including the recording of interactions with customers (Sprague, 2008). The employer, moreover, may want to determine if the employees are engaged in theft of property, misappropriation and/or disclosure of confidential information and trade secrets (*Sunbelt Rentals, Inc. v. Santiago Victor*, 2014; Nichols, 2001), as well as violations of other company policies and procedures (Sprague, 2008). The employer, moreover, may be concerned with the employees contracting computer viruses by downloading email attachments (Nichols, 2001). The employer may wish to discover if the employee is engaging in other illegal, fraudulent, or malingering misconduct, perhaps as a part of a workers' compensation investigation. The employer also may want to discover if the employee is engaged in illegal activities, such as using illegal drugs, or even if excessive alcohol use is adversely affecting a supervisor's judgment (*French v. United Parcel Service*, 1998). Surveillance, searching, and monitoring may provide the employer with concrete factual information that the employee has violated some law, company policy, or work rule so as to discipline or discharge an employee without legal liability, or for the employer to defend itself from lawsuits by employees, especially wrongful discharge and retaliation ones.

Employers, moreover, have a legal duty pursuant to the law of negligence to carefully supervise their employees; and the failure to do so in a reasonable manner may lead to liability for the tort of negligent supervision and/or retention (Cavico, Mujtaba, Samuel, and Muffler, 2016). Consequently, Carter (2016, p. 296) states that "once the private online content is accessible to the employer, it may be inferred that it would be negligent for a current or prospective employer to have failed to review and take appropriate action based on such information." Actually, one federal appeals court declared that it might be "irresponsible" for the employer *not* to monitor computer use due to "the abuse of access to workplace computers" (*Muick v. Glenayre Elecs*., 2002, p. 743). Consequently, careful and reasonable supervision may have to encompass the surveillance, searching, and monitoring of the employees at times. Therefore, such supervisory actions and the resultant obtaining of appropriate information in a proper manner should reduce the risks of lawsuits and defending lawsuits; and thus save the employer time, effort, and money in the long-term. Accordingly, as O'Gorman (2006, p. 222) points out: "Employers interested in avoiding lawsuits, and winning those already filed, are realizing what insurance companies defending workers' compensation and personal injury cases discovered long ago – surveillance is often a cost effective way to reduce expenses and losses."

Therefore, as will be seen in the case law examination, the employer's ability to demonstrate to the court one of the aforementioned legitimate reasons for the monitoring, searching, or surveillance of its employees is an important factor in avoiding liability. Yet even if there is a good reason for the employer's actions, any surveillance, searching, and monitoring must be done in a suitably non-invasive non-intrusive manner, and non-offensive manner. The next section of the article will develop the case law and review certain legal commentary to ascertain the parameters of the employer's surveillance, searching, and monitoring activities within the framework of the intentional tort of invasion of privacy.

LEGAL ANALYSIS

A person has a right to solitude and to be free from unwanted watching, prying, peeping, and spying. As such a person has a right to privacy. This right is recognized and protected by many laws, including the tort of invasion of privacy. As mentioned previously, the common law intentional tort of invasion of privacy is composed of four legal wrongs: 1) the intrusion into a person's private sphere or private affairs; 2) public disclosure to the public at-large of private facts which are offensive to a reasonable person and not of public concern; 3) the unauthorized appropriation and exploitation for commercial value of a person's name or likeness; and 4) the disclosure of information which would put a person in a false light (which is similar to the intentional legal wrong of defamation even though the facts themselves in false light need not be defamatory) (*Texas Health Resources, Trumble Insurance Company, and Texas Health Presbyterian Hospital Dallas v. Nina Pham*, 2016; *Brad Newkirk v. GKN Armstrong Wheels, Inc.*, 2016*; Sandra Gaynor c. American Association of Nurse Anesthetists and Brent Sommers*, 2015; Cheeseman, 2016; Cavico and Mujtaba, 2014; Clarkson, Miller, and Cross, 2012; Cavico, 1993; Keeton *et. al*., 1984). This four-part construction of the tort of invasion of privacy was embodied in the authoritative

Restatement (Second) of Torts (1977). However, though the tort has four parts, since there is little case law and commentary on the appropriation and false light components to the tort of invasion of privacy in the employment context, this article focuses on the first two components – intrusion and public disclosure – with prime attention given to the former.

Nevertheless, mention must be made of an important statute, the federal Electronic Communications Privacy Act (ECPA) of 1986, which regulates electronic forms of communication, including emails and cell-phone use. Pertinent to the privacy examination herein is the "business-extension exception" to the Act, which permits employers to monitor the employees' electronic communications in the ordinary course of business (Sprague, 2008). The ECPA, however, does not allow an employer to monitor the employees' personal communications unless the employees have consented to having their communications monitored by the employer (Electronic Communications Privacy Act, 1986; Sprague, 2008). Since statutes supersede the common law so long as an employer is acting within the confines of a statute – federal or state – in monitoring or testing employees the employer will be protected from common law tort liability.

A. The Tort of Invasion of Privacy

The invasion component to the intentional tort of invasion of privacy is based on an impermissible intrusion into a person's solitude, seclusion, or private sphere or place or into one's private place, affairs, or concerns wherein one has a reasonable expectation of privacy and which intrusion is regarded as highly offensive to a reasonable person (Cavico and Mujtaba, 2014; O'Gorman, 2006; *Brad Newkirk v. GKN Armstrong Wheels, Inc., 2016*; *Armstrong v. H & C Communications, Inc*., 1991; Cavico, 1993; Keeton *et. al*., 1984). The intrusion can by physical means or electronically (*Agency for Health Care Administration v. Associated Industries of Florida, Inc.*, 1996).

1. Damages

As with any intentional tort there are a wide variety of damages that the aggrieved party can recover from the defendant wrongdoer. These damages include nominal damages, actual compensatory damages (past and future so long as the latter are not "speculative"), mental anguish and emotional pain and suffering damages; and, since this legal wrong is a purposeful one, punitive damages (that is, additional damages to act as a punishment and a deterrent) (Cavico and Mujtaba, 2014; Cavico, 1993; Keeton, *et. al*., 1984). For example, in one case, a California appeals court held that even though the employer had the right to inspect the employee's office, desk, and computer, the rifling through the employee's purse was an invasion of privacy that could support a punitive damage award because the employee had a reasonable expectation of privacy regarding her personal property and the rifling was highly offensive (*Greenberg v. Alta Healthcare System, LLC*, 2004). Damages can be recovered for the outrage and mental suffering caused by the invasion as well as for the shame and humiliation that a person of ordinary sensibilities would suffer (Keller, 2013). Malice is not required for ordinary compensatory damages (Cavico and Mujtaba, 2014; Keller, 2013; Keeton, *et. al*., 1984). However, in order to sustain a recovery of additional punitive damages a showing of malice, spite, hatred, or outrageousness is required (Cavico and Mujtaba, 2014; Keeton, *et. al*., 1984). Moreover, the standard to recover mental anguish damages for this tort (as well as the tort of intentional infliction of emotional distress) is based on a person of ordinary and reasonable sensibilities and not a hypersensitive or overly sensitive person (unless the wrongdoer knows of the sensitive nature of the victim) (Cavico and Mujtaba, 2014; *State Farm Fire & Casualty Co. v. Compupay*, 1995; Keeton, *et. al*., 1984). However, for any type of the aforementioned damages for this tort as well as for intentional infliction of emotional distress it is not necessary for the aggrieved party to show any physical impact by the wrongdoer (as would be the case in a negligent infliction of emotional distress lawsuit) (Cavico and Mujtaba, 2014; *Kush v. Lloyd*, 1992; *Gracey v. Eaker*, 1999; Keeton, *et. al*., 1984).

2. Defenses

Consent is a complete defense to an intentional tort, assuming the consent is a knowing and voluntary one (Keeton, *et. al*., 1984). Accordingly, if a person consents to being watched, searched, monitored, or

contacted he or she will forego their right to sue for invasion of privacy (*Danielle Iorio v. Check City Partnership, LLC*, 2015). Waiver, that is, the knowing and voluntary giving-up of legal right, can also be a defense (Keller, 2013). Moreover, "consent and waiver may be implied or inferred from the surrounding circumstances" (Keller, 2013, pp. 987, 1018-19). For example, consent to a drug test may be inferred when the employee provides a urine sample (Keller, 2013, p. 1019). As such in one state appeals case the truck driver employee consented to take a random drug and alcohol test and to have the results and concomitant report sent to prospective employers, thereby vitiating his invasion of privacy lawsuit (*George H. Larson v. United Natural Foods West Inc*., (2014).To further illustrate, in the federal district court case of *Curtwright v. Ray* (1991), the court held that there was no invasion of privacy seclusion claim when the board of directors of a company initiated an investigation as to whether the company's president's alcohol use was affecting his performance because the president had agreed to the inspection and the company had a legitimate reason for the investigation. Assuming there are no defenses the next step in the analysis herein is to examine some of the key elements and factors with the invasion of privacy tort that can lead to legal liability.

3. The Intent Factor

Invasion of privacy is an intentional tort; as such, there is no such legal concept as a careless or negligent invasion of privacy as opposed to a negligent infliction of emotional distress tort lawsuit (in addition to the previously mentioned intentional infliction of emotional distress tort lawsuit) (Keeton, *et. al*., 1984). The intent to invade, that is, to do a purposeful act, is an indispensable element of the tort (Keller, 2013; O'Gorman, 2006). Actually, "intentionally" means that a person desires to cause the consequences of his or her act or one believes that the consequences are substantially certain to result from the act. The requisite intent, it must be emphasized, is not necessarily to cause the harm produced but rather the intent that will cause the means and the ends of invading the privacy interests of another in a manner that the law forbids (Keller, 2013; O'Gorman, 2006).

4. The Private Sphere or Private Concern Element

Initially, it is critical to point out that a legally actionable intrusion must invade a private sphere, place, or concern where a person has a reasonable expectation of privacy. Keller (2013, p. 986) in examining the Kansas case law refers to this private area a "zone of privacy" where one wants to be left alone, expects to be left alone, and reasonably expects to be left alone; and this protected "zone of privacy" also encompasses information which a person would reasonably expect to be and to remain private. Accordingly, if one is in an area or place deemed "public," or if information is deemed "public," there generally will not be a reasonable expectation of privacy; and thus no liability for any subjectively perceived "invasion" (Cavico and Mujtaba, 2014; *Allstate Insurance Co. v. Ginsburg*, 2003; Keeton *et. al*., 1984). For example, in one leading case, *I.C.U. Investigations, Inc. v. Jones* (2000), the employer as part of a workers' compensation investigation hired an investigator who conducted surveillance of the employee, videotaping the employee from roadways near his home using a telescopic lens. The videotaping, which was turned over to the employer, included the employee urinating four times in his front yard. The employee then sued his employer and the investigative firm, though the trial proceeded only against the latter. Although the jury found for the employee, assessing $100,100 in damages, the state supreme court reversed the decision, explaining that the investigation had a legitimate purpose and that the activities "carried on in his front yard could have been observed by any passerby"; and thus the intrusion was not legally actionable as an invasion of privacy tort (*I.C.U. Investigations, Inc. v. Jones*, 2000, pp. 689-90). Nonetheless, Keller (2013, p. 987) states: "Even in a public place, however, a person may keep some matters from the public gaze and maintain privacy in those matters."

Certain key privacy questions emerge in these intrusions into private place, sphere, or concern cases: first, is the activity truly private; second, whether there is a reasonable expectation of privacy, particularly in the workplace setting; and, third, if so, what is the extent of that expectation. To illustrate, in one older but leading federal appeals court case, the court held that a corporate officer reading an employee's mail, which was marked personal, but delivered to the corporate offices, would constitute an invasion of privacy based on a highly offensive intrusion into the employee's seclusion because an employee would

have a reasonable expectation of privacy in one's personal mail even in the workplace (*Vernars v. Young*, 1976). Private places would be areas where employees primarily engage in personal activities, such as locker rooms and lounges, and thus the employees would have a reasonable expectation of privacy. To search or conduct surveillance of such private places absent a very compelling reason would likely bring about tort liability. Searching offices, desks, files, and briefcases can also be problematic for the employer as they may be considered private areas by the employees, though there may be a diminished expectation of privacy if the office is shared office space (*Diana Retuerto v. Berea Moving Storage and Logistics*, 2015). Yet if the search is limited, not overly intrusive, motivated by legitimate reasons, based on reasonable suspicion, and conducted in a narrow and specific manner by proper personnel the employer may be able to conduct the search without adverse legal consequences (Cavico, 1993).

Other examples of "obviously private" activities, maintains O'Gorman (2006, p. 235), are urinating, medical examinations, and undressing. So are body functions and body fluids, adds Keller (2013, p. 1000), which are regarded as the employee's "private affairs." To illustrate, in one case a drilling rig employee who was discharged after testing positive for marijuana was awarded damages for invasion of privacy, including emotional distress damages, based on the fact that the employee was observed urinating by the employer's representative (*Kelley v. Schlumberger Tech. Corp*., 1988). However, the courts have upheld private sector drug testing when the employees have been given advance notice of the testing and the employer had legitimate reasons, obviously maintaining safety in the workplace, to be sure the employees are free from illegal drugs (*Fry v. IBP, Inc*., 1998). Even suspicion-less urine drug testing has been upheld when the employer made drug testing a condition of employment and the employer had very good reasons for the drug testing; for example, a report from an undercover agent that about 60% of the employer's workforce were using illegal drugs (*Baggs, v. Eagle-Picher Industries*, Inc.,1992). The preceding cases dealt with a private sector employer; consequently there would be no federal constitutional issues. The courts have even upheld private sector random drug testing conducted on all employees despite the fact of statements in company policy manuals that the employer would respect the personal lives of employees (*Gilmore v. Enogex, Inc*., 1994). As noted, any Fourth Amendment "search and seizure" issues where a government employer would be doing the testing might arise; but this area of constitutional law, again as noted, is beyond the purview of this article.

Some sexually oriented actions also may be construed as clearly blatant physical intrusions into private spheres where one clearly has an expectation of privacy; and thus will lead to tort liability. For example, an invasion of privacy occurs when one looks up a woman's skirt (*Michael Stancombe v. New Process Steel LP*, 2016) or when a co-worker picks up a woman's legs while she is sitting on a chair so as to look under her skirt (*Vernon v. Medical Management Associates of Margate, Inc.*, 1996). Similarly, a woman has an obvious expectation of privacy in a ladies bathroom and thus a cause of action existed when a male employee entered the ladies room and observed a female worker changing clothes (*Stockett v. Tolin*, 1992) as well as when a male "Peeping Tom" employee secretly videotaped female employees and performers in their dressing room at Disney World (*Liberti v. Walt Disney World* (1995). Consequently, Sprague (2008, p. 126) concludes that "…monitoring employees while in the bathroom or a dressing room will probably constitute a highly offensive intrusion." However, unwelcome sexual advances, unwelcome sexual touching, patting or grabbing, sexual gestures or jokes, as well as sexually offensive comments may not constitute a cause of action for invasion of privacy (*Carly Singer v. Colony Insurance Company*, 2015; *Topolski v. Chris Leef General Agency*, 2012; *Allstate Insurance Co. v. Ginsburg*, 2003; *Resley v. Ritz-Carlton Hotel Co*., 1997; Keller, 2013), though any physical touching can be grounds for the intentional tort of battery; and all can be grounds for a lawsuit for sexual harassment premised on civil rights laws (Cavico and Mujtaba, 2014). Yet one federal appeals court, citing Alabama precedent, stated that inquiries into one's sex life may be grounds for an invasion of privacy lawsuit if the inquiries are "extensive" (*Michael Stancombe v. New Process Steel LP*, 2016, p. 21).

As a general rule most work-related activities will not be considered "private" as far as the employer and the courts are concerned; and thus there will be no liability for any employer perceived intrusions (*Acosta v. Scott Labor LLC*, 2005). Nevertheless, as O'Gorman (2006, p. 237) points out: "Of course, there will

be some activities that are work-related that will still be considered private. For example, an employee who changes uniforms at work is, when changing clothes, engaged in a work-related activity, yet no one would maintain that undressing is not generally a private activity." To illustrate, in *Doe v. B.P.S. Guard Services, Inc*. (1991), the Eighth Circuit Court of Appeals held that fashion models could pursue an invasion of privacy claim against the employer of security guards when the guards videotaped the models in a dressing room, even though some of the models could not demonstrate that they were videotaped in a state of undress. To compare, in the federal district court case of *Thompson v. Johnson County Community College* (1996), there was no liability even though the employer videotaped the changing and locker rooms of security guards as part of a workplace investigation of theft because the area was not enclosed and anyone could walk into and through the area.

The employer's surveillance, monitoring, and searching may extend beyond the workplace. Employees likely will have expectations of privacy regarding their off-the-job activities. As such, the employer must have legitimate business reasons for such conduct. Consequently, these employer actions can give rise to lawsuits for invasion of privacy if the employer lacks a strong reason and the methods are unreasonable and offensive (Cavico, 1993). Yet if the surveillance or monitoring is in a public place there should be no liability because the employee will not have a reasonable expectation of privacy (Cavico, 1993).

When the surveillance is of the employee inside of his or her home the legal situation becomes even more problematic, particularly if vision-enhancing equipment is used. Compare the case of *Salazar v. Golden State Warriors* (2000), where the court rejected an invasion of privacy claim even though the employer's investigator used a high-powered, infrared, night vision, telescoping device to take footage of an employee using drugs in his sports utility vehicle in a dark parking lot, with *Saldana v. Kelsey-Hayes Company* (1989), where the court said that the use of such a comparable device to view an employee, suspected of malingering, in the interior of his home could be objectionable on privacy grounds. Yet a very strong and legitimate business reason may legitimize an intrusion into the employee's home (Cavico, 1993).

The prevalence today of social media presents another challenge to the law. Now, one would think that an employee might consider his or her social media postings as private. Yet, two federal district court cases are most instructive; and thus should serve as a warning to employees. In one case the former employer accessed and used the employee's personal Twitter and Facebook accounts without the employee's authorization; but the court dismissed the employee's invasion of privacy claim explaining that matters discussed on these social media accounts were not private (*Maremont v. Fredman Design Group, Ltd*., 2011). In the other case the plaintiff employees contended that their manager accessed a secure password protected chat room on Myspace where the employees were complaining about their employer; but a jury ruled against the plaintiff employees on their invasion of privacy claim because the jury determined that regardless of the unauthorized access the plaintiffs did not have a reasonable expectation of privacy for their chat room communications (*Pietrylo v. Hillstonne Restaurant Group*, 2009). These cases clearly underscore the maxim that nothing on social media is truly private. Yet as a result of these cases several states have promulgated statutes that prohibit employers from requesting social media passwords from applicants and potential employees (Mgrditchian, 2015). Of course, these laws may not protect current employees or prohibit the employer from obtaining social media information from a third party with access or knowledge of access. Moreover, Mgrditchian (2015, p. 130) points out that "…many companies have enacted policies that directly ban any use of social media during working hours. Such workplace policies would diminish the expectation of privacy of employees who decide to tweet or post on Facebook, because it is likely that companies that ban such activities will be contemporaneously monitoring Internet use to ensure that the policy is being followed by its employees."

The personnel information and records that the employer obtains and maintains as part of its human resources function, including medical records of the employees, will usually not be considered private for the intrusion aspect of the invasion of privacy tort so long as the information relates to the employer's management of the workplace or is otherwise public information, for example arrest and conviction records (Keller, 2013). However, the information may be deemed private regarding others; and thus its

disclosure could trigger the disclosure of private facts component to the invasion of privacy tort, which will be succinctly examined in a forthcoming section to this article.

5. The Offensiveness of the Means Element

Surveillance, monitoring, and searches do not automatically give rise to the tort of invasion of privacy. These actions may be reasonable, non-intrusive, not objectionable to the "reasonable person," and for good reasons. For tort liability to arise the means used to intrude or pry into the private sphere or private concern must be deemed outrageous or highly offensive or highly objectionable to the reasonable person (O'Gorman, 2016; Cavico and Mujtaba, 2014; Keller, 2013; Clarkson, Miller, and Cross, 2012; Cavico, 1993; Keeton *et. al*., 1984). To illustrate, Sprague (Spring, 2008, p. 403) points out that an employer "prying – in detail – about an employee's sex life" has been found by the courts to be highly offensive to a reasonable person. To further illustrate, in the case of *Blackwell v. Harris Chemical North America, Inc*. (1998), the federal district court ruled that the employer's attempt to obtain confidential medical information about an employee who requested a medical leave by badgering and harassing a nurse at the treating physician's office stated a claim for intrusion on seclusion because the information was private. The case is also important because it illustrates the point that even if the employer may have had a legitimate need for the information, the means used, as ruled the court, was unreasonable and offensive (*Blackwell v. Harris Chemical North America, Inc*. (1998).

6. The Place of Surveillance

Another factor in determining liability for surveillance is the place of surveillance (Cavico, 1993). Accordingly, as emphasized by Gorman (2006, p. 254), this key fact is whether the employer conducted the viewing, monitoring, or surveillance from a "lawful vantage point." Consequently, watching or photographing a person through the windows of his or her residence could be an impermissible intrusion as well as a possible trespass (*Dana Retuerto v. Bera Moving Storage and Logistics*, 2015). Even if the surveillance is conducted by means of telescopic or image-enhancing equipment, and even if the employer had a good reason for the surveillance, if the employer was in place that the employer did not have a right to be the courts may find the employer liable for invasion of privacy. For example, if a manager or supervisor enters the employee's trailer home without permission, even for a good reason, such as to see if the employee had a drinking problem and thus was not suitable for a supervisory position (*Love v. Southern Bell Telephone & Telegraph Co*., 1972), or if there was a trespass and the employee was watched in his/her home by investigators using binoculars who also eavesdropped on the employee's spouse (*Souder v. Pendleton Detectives, Inc.*, 1956), there would be legal violations.

7. The Legitimate Reason Element

The employer must also have a legitimate job-related reason for the surveillance or monitoring. Moreover, as O'Gorman (2006, p. 264) points out: "This factor helps insulate most employers from liability for surreptitious physical surveillance of employees because it is unusual for an employer to conduct such surveillance for illegitimate reasons, and the motive will usually be considered legitimate so long as it is work-related." The supervisor of an employee who tries to obtain her medical records to discredit her and to spread rumors that she is a lesbian because she rebuffed the supervisor's sexual advances is clearly not a legitimate business reason (*Lankford v. City of Hobart*, 1994).

As noted, many valid reasons can be offered as "legitimate" ones for surveillance and monitoring, such as promoting productivity and efficiency at work (*Thomas v. General Electric Company*, 1962); and these legitimate reasons can even encompass off-the-job surveillance of employees, for example, investigating wrongdoing by employees (*DeLury v. Kretchner*, 1971) or defending a legal claim asserted by an employee (*Ellenberg v. Pinkerton's, Inc*., 1973). However, even if the employer has such a legitimate reason, the employer still must be careful that the means of surveillance, monitoring, and searching are not highly offensive to the reasonable person. Consequently, even if the employer has a legitimate reason for the surveillance the means involved may go beyond the bounds of decency and thus trigger tort liability. For example, in the federal district court case of *Acuff v. IBP, Inc.* (1999) the employer as part of a workplace investigation as to theft installed a camera in the ceiling tiles of the nurse manager's office because certain items were disappearing from the office. That rationale for the surveillance could be

construed as a legitimate one. However, the office was also used for employee medical examinations, which the nurse manager and the employee who viewed the videotapes were aware of, and this knowledge was imputed to the employer, thereby resulting in liability for invasion of privacy for the surreptitious surveillance (*Acuff v. IBP, Inc.* (1999). To compare, in one federal district court case, *Corian Branyan v. Southwest Airlines Co.* (2015), the employer, an airline company, was attempting to contact an employee, a flight attendant on paid-leave with a wrist injury, to determine her status and availability for work. The employer attempted to contact her 25 times to no avail. As a result, the employer contacted the local police to find her, providing to the police her name, home address, and employment status. The employee sued for invasion of privacy contending that such an "unfair intrusion" led to the police coming to her residence. The court, however, denied her claim, stating: "Those allegations are insufficient to constitute a cognizable invasion of privacy claim. A person's name, home address, and employer are hardly facts of a highly personal or intimate nature. Nor can a brief home visit from a police officer properly be characterized as an unreasonable, substantial or serious interference with plaintiff's privacy" (*Corian Branyan v. Southwest Airlines Co*., 2015, pp. 10-11). The court also pointed out that "…legitimate business reasons for the reasonable collection or dissemination of private employee information are not actionable" (*Corian Branyan v. Southwest Airlines Co*., 2015, p. 10).

Therefore, in the employment sector or otherwise there are many factors to consider; and consequently the "totality of the circumstances" must be considered (Keller, 2013, p. 987). A key factor to determining the "offensiveness" element, maintains Keller (2013, p. 993), is whether the "employer's legitimate business interest outweighed the employee's privacy interest." Similarly, Sprague (2008, p. 126) emphasizes that "whether an employer's invasion of privacy is highly offensive depends on whether the employer has a legitimate business interest justifying the intrusion. Consequently, a jury may be necessary in order to determine the application of this objective "reasonable person" test; that is, the jury as trier of fact must decide if such a hypothetical reasonable person would be highly offended and outraged by the intrusion even though the employer may have had a good reason for certain information (O'Gorman, 2006, pp. 261-62).

8. Electronic Monitoring

Another challenging area of the law is the application of the tort of invasion of privacy to the electronic monitoring of employees. The maxim is that "the law is always trying to catch up to technology." And this old saying is never been more true than today when the old English common law tort of invasion of privacy (likely judicially promulgated back in Middle Ages during the reign of the King Henry I and King Henry II) is applied to modern electronic monitoring, particularly in the workplace. Employers today in the global "virtual" economy routinely provide to their employees Internet access and email and other forms of electronic communication and access. Employers have the technical ability to electronically monitor these modalities as well as phone calls and text messages. Robertson and Kanaga (2008) describe two basic types of computer monitoring:

One type of computer monitoring program often used by employers is a 'packet sniffer.' This is a program that connects to a particular computer network and then views all the information that passes over that network. Packet sniffer programs can monitor the Internet activity on an employee's network, including the Web sites that the employees visit, the contents of their e-mails, and what information is being downloaded from the Internet….Another form of computer surveillance used by many employers is desktop monitoring. When an employee logs into his or her computer, a signal is transmitted that is intercepted by the program. The program then replicates what the employee sees on his or her computer screen at the moment that signals are transmitted (p 30).

To further illustrate the rapid, extensive, and intrusive new technology *Bloomberg Businessweek* (Khrennikov, 2016) reported that a Russian security company, called InfoWatch, has now developed a technology that will enable employers to eavesdrop on cell phone calls made on their premises, including the employees' (presumably) private personal calls. The objective of the technology is to help employers prevent the misappropriation and transmission of confidential business information and commercial and trade secrets (Khrennikov, 2016). Privacy is maintained, supposedly, due an initial screening mechanism

in the technology that is performed by a computer, based on software developed first for the KGB, that scans and analyzes the calls for key words that might cause business concern, such as "brokerage account" and "share offering" but not "football" or "sex" (though the system could be programmed for these latter words) (Khrennikov, 2016, p. 32). If suspicious words are found then the text fragments can be sent to the company's security office for further investigation (Khrennikov, 2016). This technology is called, and is being marketed as, the new "hot ticket" for companies that want to protect confidential business information, though of course there are privacy and legal liability concerns (Khrennikov, 2016, p. 31). The company is still testing the technology; and no price has been set for the new technology yet (Khrennikov, 2016). Employers contemplating the use of this new technology should take heed of an older case where the court held that the employer violated a precursor to the Electronic Communications Privacy Act when it allowed employees to use phones for personal calls as well as for work, stated that monitoring would occur but assured the employees that their calls would be monitored only to determine if they were for business purposes; yet nonetheless a supervisor listened in to a personal call between an employee and a friend (*Watkins v. L.M. Berry Co.*, 1983).

Employers also have legitimate reasons for engaging in electronic monitoring as well as the surveillance of employees. As noted earlier, employers have a duty to protect confidential information and trade secrets and to prevent defamation, cyber-bullying, discrimination, and harassment in the workplace. An interesting and instructive case dealing with alleged misappropriation of trade secrets by a former employee is the federal district court case of *Sunbelt Rentals, Inc. v. Santiago Victor* (2014). As part of its investigation into misappropriation the employer reviewed the former employee's text messages on the iPhone which the employer had previously issued to the employee. The former employee sued for invasion of privacy for the allegedly impermissible intrusion, claiming that he had a reasonable expectation of privacy in the text messages. However, the court denied his claim, stating firstly that the device belonged to the employer; and secondly that while he may have had a subjective expectation of privacy it was not a reasonable one because the employee personally caused the transmission of his text messages to the iPhone by "syncing" his new devices to his Apple account without first linking his former employer's iPhone (*Sunbelt Rentals, Inc. v. Santiago Victor*, 2014, pp. 19-20). The court further explained: "As such, even if he had *subjectively* harbored an expectation of privacy in his text messages, such expectation cannot be characterized as *objectively* reasonable, since it was (former employee's) conduct that directly caused the transmission of the text messages to (the former employer) in the first instance" (*Sunbelt Rentals, Inc. v. Santiago Victor*, 2014, p. 20 (emphasis in original)). In addition to underscoring the critical distinction between a subjective and an objective expectation of privacy the case also serves as a reminder of the "perils and pitfalls" of technology on privacy. Employers who wish to monitor the text messages of their employees must be careful too. Since employees may have a reasonable expectation of privacy regarding their text messages (*Quon v. Arch Wireless Operating Company*, 2008), employers should clearly notify employees that their text messages will be monitored and also obtain an express acknowledgement from the employees as to the monitoring (Sprague, 2008).

Employers are also very concerned about their reputations – "virtually" and otherwise. Schoening and Kleisinger (2010, p. 288) pointed to a 2009 survey by one of the big accounting firms which indicated that 60% of employers surveyed believed that they had a "right to know" how employees portrayed their organizations online. And the advent and extent of social media sites and networks provide the means for employers to monitor employees' online statements and activities. Consequently, employers rightfully contend that they have legal, ethical, and practical reasons to monitor their employees' electronic communications as well as social media sites. Yet, naturally, employers want to avoid liability for invasion of privacy. The aforementioned Electronic Communications Privacy Act (1986) affords the employer a great deal of protection since the employer can access and retrieve information on its computer systems or the employee otherwise gives consent to access. However, monitoring social media sites is another matter indeed, particularly when the aforementioned survey also indicated that 53% of employees surveyed believed that "social networking pages are none of the employer's business" (Schoening and Kleisinger, 2010, p. 288).

Yet there is a concern about the potential liability to the employer under tort law. The fact that the employer provided the email system to the employees emerges as the critical factor in determining liability. For example, the courts have held that an employee has no reasonable expectation of privacy in email communications that the employee voluntarily made on the company's email system (*Symth v. Pillsbury Co*., 1996), even when messages are stored in a password-protected location on the employees' computers at work (*McLaren v. Microsoft*, 1999). The courts have even held that an employer can monitor of its independent contractors, holding that the fact that the person was not technically an "employee" was irrelevant; and thus again the key fact is that the employer provided the email system to the independent contractor (*Fraser v. Nationwide Mutual Insurance Co*., 2004). However, to compare, in the federal district court case of *Ali v. Douglas Cable Communications* (1996), the court drew a distinction between the employer's monitoring of its customer-service employees' work-related calls for supervision and training purposes, which were deemed permissible intrusions, versus the employer's monitoring and recording of the employees' personal calls without prompt notification, which actions were held to violate their right to privacy since their expectation that the personal calls would remain private was a reasonable one.

Another complicating factor arises when employees are allowed to work at home, that is, they are "telecommuting" employees. As such, Keller (2013, pp. 994-95) points out that "as home and office life merge, employers can more easily argue for a business need to inquire into or monitor employee behavior away from the employer's business site." Sprague (2008, p. 130) adds that "with the merger of home and office life, employers can more easily argue for a business need for monitoring employee conduct offsite. A growing number of employees now work in the virtual workplace – not in the office, but on the road or home. Since there is less face-to-face interaction among workers, there is a greater reliance on electronic communications." Nichols (2001, p. 1593) concludes that telecommuting "…for the employee, is a gray area in the realm of privacy. Once he logs onto his employer's network, his employer may have access to his 'private files' stored in his home computer. The employer should not have a legitimate business need to examine these files, but nevertheless, the employee may be vulnerable to employer snooping." Further complications arise when the employee is not technically a "telecommuting" one but rather the employer has given the employee a computer for home use so the employee can conduct some of the employer's business from home (Nichols, 2001). The employee of course will have access to the employer's business systems but he or she may use this home computer provided by the employer for personal use, thereby raising privacy questions. Key factors, therefore, in the legal analysis would be whether the employee had a reasonable expectation of privacy regarding the online information, the legitimacy and strength of the reason by the employer to obtain the information, the means used by the employer to access the information, and whether the employer's business need superseded the employee's privacy interest.

Moreover, employers today can even monitor the physical movements of their employees by means of Global Positioning System (GPS) technology. Privacy issues can arise when the employer used GPS systems to keep track of employees, vehicles, and equipment; but the employer may have legitimate reasons to do so. Sprague (2008, pp. 130-31) notes that "many cell phones are GPS-enabled, allowing employers to track the whereabouts of the phones they provide to employees, as well as the employees carrying those phones." One leading GPS decision is the federal district court case of *Elgin v. St. Louis Coca Cola Bottling Co.* (2005), where the court held that the employer did not commit an invasion of privacy intrusion tort by engaging in the GPS monitoring of an employee in a company-owned vehicle even on the employee's personal time. Note that the preceding case is a private sector one; and thus the result may be different when the government as employer or otherwise engages in GPS tracking due to Fourth Amendment concerns (Keller, 2013, pp. 1015-16).

Monitoring, therefore, involves a consideration of the means of the monitoring and the employer's interest in doing the monitoring as well as the relevance of the information received to the employer's interest. If the monitoring is aimed at the employee's private or personal information the likelihood increases that the monitoring will be an illegal intrusion unless the employer has a very compelling reason for the monitoring.

B. The Tort of Public Disclosure

The public disclosure component of the invasion of privacy tort is based on the unauthorized public disclosure by a person of private facts regarding an individual that a reasonable person would find highly offensive, objectionable, or embarrassing and the matter is not of legitimate public concern (*Jane Doe v. Bernabei & Wachtel, PLLC,* 2015; Cavico and Mujtaba, 2014; Clarkson, Miller, and Cross, 2012; Sprague, Spring, 2008; Cavico, 1993; Keeton *et. al*., 1984). It is important to note that this legal wrong is different from defamation where the negative material about a person must be false; rather, with public disclosure there may be liability pursuant to this privacy tort even if the information is true, because the information is private and not a matter of public concern (Cavico and Mujtaba, 2014; Clarkson, Miller, and Cross, 2012; Keeton *et. al*., 1984). A key question here, as with the intrusion aspect of the tort, is whether the information disclosed was highly offensive to a reasonable person. For example, in the federal district court case of *Jennifer Pwlaczyk v. Besser Credit Union* (2014), when the vice-president of a credit union was discharged the CEO of the credit union emailed other credit union CEOs to inform them that the VP was no longer employed at the company. The former VP then sued pursuant to the public disclosure of private facts component to the tort of invasion of privacy. The court, however, denied the VP's claim for the following reasons: only a small group of CEOs was contacted; there was no evidence that the information would become public knowledge; there was no evidence that the VP would not be able to find suitable employment in her field; and, most importantly the CEO just said that the VP was no longer employed at the company; and the communication by the CEO "does not disclose the nature of the separation or any reasons behind it" (*Jennifer Pwlaczyk v. Besser Credit Union* (2014, p. 17). Another key question is whether the private information was sufficiently disclosed to rise to the level of a "public disclosure." As such, disclosure to a single person or even a small group of people will not be adequately "public," for example, when a company's human resources department disclosed the personal bank account information of an employee, who was having a pay dispute with his company, to his supervisor (*Anand Venkatrman v. Allegis Group, Inc.*, 2015).

If information is deemed to be public or in the public record then one can examine and transmit such information without violating tort law (*Markovitch v. Panther Valley School District*, 2014; Keller, 2013). Yet if information about a person is deemed to be "private" tort liability for invasion of privacy may ensue. Yet particularly in the employment context ascertaining whether certain information is private or public is a difficult task indeed, especially with the advent of highly developed technologies. Keller (2013) further explains:

So while it may be clear that you do not intrude on a person's seclusion by observing her on a public street, it is not clear, for example, whether you invade her privacy by tracking all her movements on public streets for a long period of time with GPS technology. Whether a matter or information is private can also be more difficult to discern in the employment context where employers and employees share physical space, property, and information. Determining, for example, whether employees can expect privacy in personal phone calls made on employer-owned phone equipment or in personal files on company-owned computers, involves complex, fact-specific inquiries (p. 987).

One of the first public disclosure of private facts employment cases is the 1990 decision by the Illinois court of appeals in *Miller v. Motorola* (1990) where the employer revealed to many co-workers that the plaintiff employee had a mastectomy, thereby resulting in tort liability for invasion of privacy. Another leading case is the Colorado Supreme Court case in *Ozer v. Borquez* (1997) where tort liability was premised on a law firm partner's telling other employees that a law associate was homosexual, that his domestic partner had been diagnosed with AIDS, and that he needed to get tested to determine if he was HIV positive. Other examples would be disclosure of details of sexual relations and intimate private conduct (Sprague, 2008). The aforementioned examples would be highly offensive to the reasonable person. Finally, it should be pointed out that the public disclosure tort of course requires that the private information be made public, but the intrusion aspect of invasion of privacy "…does not depend upon any publicity given to the person whose interest is invaded or to his affairs" (*Dawn Hahn v. Cynthia Loch,*

L.P.N., Lehigh Family Practice Associates, LLC, and Leroy Hahn, 2016, p. 15, citing the Restatement (Second) of Torts).

Overall, invasion of privacy in the employment context and otherwise is a very challenging area of the law. As seen from the preceding analysis, there is no clear, exact, and definitive test to determine if an impermissible intrusion occurred. Generally, though, there must be an offensive intrusion into a person's private sphere or concern where one has a reasonable expectation of privacy. The resulting very fact-specific and complex analysis must consider the following criteria, to wit: the presence of a private sphere, place, or concern, the degree and nature of the intrusion, the offensiveness of the intrusion, particularly regarding community norms and mores as to offensiveness, the expectations of privacy – subjectively to the employee whose privacy was allegedly invaded as well as objectively to the "reasonable person," and the employer's reasons, objectives, and motives for the intrusion. The next section to the article will further discuss the implications of this tort in the employment section, focusing on the ramifications for management.

IMPLICATIONS FOR MANAGEMENT

A major legal, ethical, and practical area of management concern is the extent to which the employees' right to privacy is protected in the workplace. The authors wish to emphasize initially two important points: first, not all surveillance, searching, and monitoring are legally actionable; second, invasion of privacy cases – in employment and otherwise – are very fact-specific types of cases; and thus the result depends on the circumstances in the individual case. The courts seek to balance the legitimate interests of the employer with the employee's right to privacy. As one federal court stated, citing Massachusetts precedent, in order to determine whether a privacy violation occurs, "…the employer's legitimate interest in determining the employee('s) effectiveness in (her) job should be balanced against the seriousness of the intrusion on the employee('s) privacy" (*Emily Billing v. Martha's Vineyard Public Charter School*, 2014, p. 14). Similarly, another court stated: "In an employment relationship, courts will balance the legitimacy of an employer's need to obtain personal information against the seriousness of the intrusion into the employee's privacy" (*Corian Branyan v. Southwest Airlines Co*., 2015, p. 10). A key question, therefore, is whether the employer's legitimate need for certain work-related information outweighs the employee's interest in privacy.

As emphasized, most work-related activities will not be deemed to be sufficiently "private" as far as the employer is concerned, thus obviating tort liability. Generally, therefore, employees do not have the right to be free from surveillance in the workplace – surreptitious or otherwise. As O'Gorman (2006, pp. 258-59) explains: "Because the employer has a lawful right to be at its own workplace, the employer has the right to view anything that is in plain view from such a vantage point." Keller (2013, p. 993) similarly states: "Employers generally own and control the workplace, and thus are to some level responsible for what occurs there. Employers must be able to maintain and control their property and monitor employees to ensure they perform their jobs in a satisfactory, efficient, and safe manner. Because of these interests, different expectations of privacy will exist in the workplace than in other contexts." For example, since employers typically own their computer systems it will be very difficult for an employee to successfully claim that he or she has a reasonable expectation of privacy regarding such computer use. Moreover, employees would not have a right to privacy in offices, even if "their" offices, since the offices belong to the employer and can be accessed by the employer's managers and supervisors, even if the access is accomplished by video surveillance (O'Gorman, 2006, pp. 258-59). To illustrate, in the federal district court case of *Marrs v. Marriot Corp*. (1992) the employer monitored the office and desk of an employee security investigator with his permission as he believed that someone was wrongfully accessing his files. The employer then observed another employee attempting to pick the lock of a desk drawer with a paper clip. The employee was fired and sued for invasion of privacy; but the court denied the claim ruling that the plaintiff employee did not have "a reasonable expectation of privacy in an open office" (*Marrs v. Marriot Corp*., 1992, p. 283).

Nonetheless, even in the workplace and during the work relationship employees are accorded a protected sphere of privacy and seclusion. Some areas of the workplace are private; and thus the employees can have a reasonable expectation of privacy, for example, as pointed out, going to the bathroom, dressing and undressing at work, and regarding personal items contained in their briefcases, desks, and lockers. To illustrate, in one case a court found that the employee had a reasonable expectation of privacy regarding her locker, even though it was provided by the employer, because the contents of the locker were secured by the employee's own lock (*K-Mart Corporation v. Trotti*, 1984). As such, to impermissibly intrude into this private sphere without a very strong countervailing reason can bring legal liability on the employer in the form of an intentional tort invasion of privacy lawsuit as well as other legal actions by the aggrieved employees.

However, for there to be an illegal invasion the employee, as any person, must have a reasonable expectation of privacy. As such, in order for the employee to prevail on an invasion of privacy lawsuit based on the employer's allegedly intrusive actions the employee must be able to show that he or she had a reasonable expectation of privacy. "Reasonable," as emphasized, is measured by an objective – "reasonable person" standard and not by the employee's subjective feelings. Accordingly, if the employee is in a public place and can be viewed from such a location there typically will not be an invasion of privacy, even if the employee is photographed or videotaped. Moreover, if an employee is informed by management that he or she will be watched, searched, subject to surveillance, or monitored – physically or "virtually" – it will be very difficult for the employee to claim that his or her expectation of privacy was a "reasonable" one – whether on- or off-the-job, thereby typically obviating tort liability on the part of the employer for any perceived "invasion." Conversely, if the employee is not notified by management of certain monitoring or surveillance it is more likely that the employee will be able to sustain an invasion of privacy lawsuit based on intrusion. A notification policy must be thorough, clear, and specific and communicated to the employees. Moreover, it should emphasize that even certain activities which might be considered "private" will be viewed. O'Gorman (2006) warns of the risk of having too general a policy, to wit:

Even with a general surveillance policy that is adequately emphasized, surveillance in a location like a restroom stall would most likely not defeat a claim…because, even with the policy, a reasonable employee might not believe his or her activities in the bathroom stall were at serious risk of being exposed by the employer. A general statement that the employer has the right to conduct surreptitious surveillance of an employee at any location would probably not make unreasonable an employee's expectation not to be viewed in the bathroom stall. An employer could, however, potentially defeat a claim by issuing a policy clearly indicating surveillance will take place in the bathroom stall (pp. 252-53).

Allegations of invasion of privacy can also arise during the application, screening, interviewing, and testing process of the employment relationship. As such, employers must be careful as to what questions they can ask so as not to be perceived as intruding on a job applicant's private sphere. For example, asking about an applicant's sexual orientation or political affiliations, or religious beliefs might well be construed as improper questions, particularly if asked in a selective manner. Consequently, any and all questions and testing must have a reasonable connection to the job or position and must be asked in a non-discriminatory manner.

The employee's expectation of privacy and whether such an expectation is a reasonable are seminal issues in invasion of privacy cases. Accordingly, Noyce (2011) emphasizes that the key to avoiding liability for invasion of privacy is for the employer to be aware of its employees' expectations of privacy to "manage" those expectations in a proper manner. Noyce (2011) explains:

When an employer is successful in this endeavor, it will not be subject to liability for violating employee privacy rights because the employee will not have a reasonable expectation of privacy on which to base a claim. If an employer, public or private, can successfully manage its employees' expectations of privacy, courts will be less inclined to find the employer liable, and the employee will be less likely to file a suit against the employer in the first place. From the employer's perspective, managing employees' expectations of privacy is the first line of defense against liability for alleged infringement of employee

privacy; it also is in the best interest of the employee if the parties have similar expectations with regard to employee privacy (p. 62).

In the next section to the article we provide recommendations to help managers avoid liability for the intentional tort of invasion of privacy.

RECOMMENDATIONS FOR MANAGEMENT

Based on the preceding legal analysis and discussion the authors offer the following suggestions to management to help manage the employees' expectations of privacy; and thus to avoid liability for invasion of privacy lawsuits:

- Develop surveillance and monitoring policies that are clear and definite.
- Develop surveillance and monitoring policies that are fair and dignified and respectful to the employees.
- Establish a precise privacy policy that clearly, thoroughly, explicitly, and specifically notifies the employees how, when, and what will be watched, monitored, tested, searched, or subject to surveillance, especially regarding activities and/or areas that could be deemed to be "private."
- Train managers, supervisors, and employees as to the company's privacy policies.
- Make sure that managers and supervisors do not deviate from the firm's formal privacy policies (Noyce, 2011).
- Publish these policies in employee handbooks and codes of conduct.
- Require employees to sign waiver or consent forms as to surveillance and monitoring as conditions of employment.
- Obtain a receipt from the employee that he or she has read and understands the surveillance and monitoring policy.
- Let the employees know that not only emails but also text messages may be monitored.
- Inform employees that the email system is the sole property of the employer and is to be used only for business purposes.
- Inform employees not to expect email on their office computers to be considered as private communications.
- State that security measures on email systems, such as password and message-delete mechanisms, do not prevent the employer from accessing or retrieving emails and that the employer may override individual employee passwords or codes (Howard, 2008).
- Tell employees to make personal calls from their personal cell phones and not the employer's office phones.
- Tell employees not to conduct personal activities on the company's computer network.
- Inform the employee that if he or she brings a personal laptop to work, which is then connected to the employer's system, that such use may be monitored by the employer.
- Inform the employees that they should tell their family members, friends, and co-workers not to send any personal emails or make any personal calls to the employee's office computer and/or phone.
- Have clear, strong, legitimate, and demonstrable reasons for any surveillance, searching, testing, and monitoring of employees.
- Regarding surveillance of off-the-job activities, note that the counsel of the National Institute of Business Management states: "If an employee's off-duty activity puts your company in legal or financial jeopardy, courts will be more willing to let you regulate it" (Schoening and Kleisinger, 2010, p. 320).
- If the surveillance or monitoring is to take place offsite Sprague (2008, p. 132) advises that the business reason be not only legitimate but also "substantial."

- Only search an employee's office or desk for a legitimate work-related reason, such as to find a necessary file or materials pertinent to work, or when there are reasonable grounds to suspect that the employee is involved in some type of work-related misconduct.
- Do not engage in any overbroad, unnecessary, irrelevant, or unsupervised searches, for example, into the employee's personal property, such as purse or jacket pocket, or an investigation into the employee's sexual practices.
- Limit disclosure of private information concerning employees only to managers, supervisors, and others who have "a clear need to know" (Howard, 2008, p. 522).
- Inform managers and supervisors that any improper sharing of private information concerning the employees will subject them as well as the company to potential invasion of privacy lawsuits (Howard, 2008).
- Remember that "the employee…need not be terminated in order to assert a…claim for violating the employee's right to privacy" (Noyce, 2011, p. 39).

The authors trust that these recommendations and suggestions will help managers to avoid liability for the intentional tort of invasion of privacy.

SUMMARY

In today's workplace employers do obtain and collect a great deal of information about their employees; and employers have quite legitimate reasons to do so. However, employers also have very genuine concerns about protecting themselves from legal liability under federal and state laws – statutory, regulatory, and common law. As such, the field of employment law is a vast one as surely is the area of privacy law. This article has dealt with one narrow aspect of employment and privacy law – the examination, explication, application, and illustration of the common law intentional tort of invasion of privacy in the private sector workplace. The authors dealt with two components of the tort – intrusion into seclusion and public disclosure of private facts. Moreover, the focus was on the former as well as on the private sector, thus obviating any detailed discussion of constitutional law privacy protections that public sector employees could assert against their government employers. However, some public sector cases were used as illustrations. The authors analyzed the two aforementioned components of the tort of invasion of privacy by examining case law and legal and management commentary. The authors then discussed the implications of their legal analysis for management; and made pertinent recommendations to management in order to avoid liability.

While employers can have good reasons as well as the legal right to engage in monitoring, searching, and surveillance of their employees that legal latitude is not without bounds. The old common law tort of invasion of privacy is one important legal means to limit the employer's surveillance, searching, and monitoring of its employees. "Reasonableness" is a key factor in this legal analysis as it is with much of tort law. In essence, the courts apply a "reasonableness" test to the employer's conduct in order to determine if an employer intrusion into the employee's privacy, even if for a good reason, would be highly offensive to the reasonable person. The more offensive the means of intrusion the stronger the employer's justification must be. These employment privacy cases, therefore, are very fact-specific; and consequently each case is therefore decided on its own facts and circumstances. One can sense that the courts are seeking to balance in an equitable manner the legitimate business and employment interests of the employer against the employee's interests in maintaining and safeguarding his or her privacy and the reasonableness and offensiveness of the intrusion into the employee's privacy.

The authors stress that surveillance, searching, and monitoring policies must be not only legal, but also fair, dignified and respectful to the employees. In addition to avoiding legal liability acting in such a legal and ethical manner is in the long-term interest of the employer in attracting and maintaining high quality employees as well as to achieving and maintaining a good reputation with clients, customers, shareholders, the community, and the legal system. The authors' goal, therefore, has been in the privacy

and employment context herein to assist managers to achieve a legal, fair, ethical, and practically efficacious workplace.

BIBLIOGRAPHY

Acosta v. Scott Labor LLC, 377 F. Supp. 2d 647 (District Court for the Northern District of Illinois 2005).

Acuff v. IBP, Inc., 77 F. Supp. 2d 914 (1999).

Agency for Health Care Administration v. Associated Industries of Florida, Inc., 678 So.2d 1239 (Florida Supreme Court 1996).

Ali v. Douglas Cable Communications, 929 F. Supp. 1362 (District Court for the District of Kansas 1996).

Allstate Insurance Co. v. Ginsburg, 863 So.2d 156 (Florida Supreme Court 2003).

Anand Venkatrman v. Allegis Group, Inc., 2015 U.S. Dist. LEXIS 122409 (District Court for the District of Maryland 2015).

Armstrong v. H & C Communications, Inc., 575 So.2d 280 (Florida District Court of Appeal 1991).

Baggs, v. Eagle-Picher Industries, Inc., 957 F.2d 268 (Sixth Circuit Court of Appeals1992).

Blackwell v. Harris Chemical North America, Inc., 11 F. Supp. 2d 1302 (District Court for the District of Kansas1998).

Brad Newkirk v. GKN Armstrong Wheels, Inc., 2016 U.S. Dist. LEXIS 29858 (District Court for the Northern District of Iowa 2016).

Carly Singer v. Colony Insurance Company, 147 F. Supp. 3d 1369 (District Court for the Southern District of Florida 2015).

Carter, Ralph (2016). Too Much Information: The Need for Stronger Privacy Protection for the Online Activities of Employees and Applicants. *Journal of Civil Rights and Economic Development*, Vol. 28, pp. 291-318.

Cavico, Frank J. (Fall 1993). Invasion of Privacy in the Private Employment Sector: Tortious and Ethical Aspects. *Houston Law Review*, Vol. 30(4), pp. 1263-1346.

Cavico, Frank J. and Mujtaba, Bahaudin G. (2014). *Legal Challenges for the Global Manager and Entrepreneur* (Second Edition). Dubuque, Iowa: Kendall Hunt Publishing Company.

Cavico, Frank J., Mujtaba, Bahaudin, G., Samuel Marissa, and Muffler, Stephen (2016). The Tort of Negligence in the Employment Sector – Negligent Hiring, Supervision, and Retention – and Recommendations for Managers. *American Journal of Business and Society, in-press*.

Cavico, Frank J., Mujtaba, Bahaudin G., and Muffler, Stephen (2014). Criminal Background Checks in Employment: An Unfolding Legal Quandary for Employers. *Journal of Criminal Law and Criminal Justice*, 2(1), pp. 41-103.

Cavico, Frank J., Mujtaba, Bahaudin G., Muffler, Stephen, and Samuel, Marissa (2013). Social Media in the Workplace: Legal, Ethical, and Practical Considerations for Management. *Journal of Law, Policy, and Globalization*, Vol. 12(1), pp. 1-46.

Cheeseman, Henry (2016). *Business Law* (Ninth Edition). Boston, Massachusetts: Pearson Education, Inc.

Clarkson, Kenneth W., Miller, Roger LeRoy, and Cross, Frank B. (2012). *Business Law: Text and Cases* (Twelfth Edition). United States: South-Western, Cengage Learning.

Comprehensive Care Corporation v. Katzman, 2010 U.S Dist. LEXIS 35410 (District Court of Florida 2010).

Corian Branyan v. Southwest Airlines Co., 105 F. Supp.3d 120 (District Court for the District of Massachusetts 2015).

Courtney R. Robbins v. The Trustees of Indiana University and Clarian Health Partners, Inc., 45 N.E.3d 1 (Indiana Court of Appeals 2015).

Curtwright v. Ray, 1991 U.S. District LEXIS 12429 (District Court for the District of Kansas 1991).

Danielle Iorio v. Check City Partnership, LLC, (2015 Nev. LEXIS 658 (Supreme Court of Nevada 2015).

Dawn Hahn v. Cynthia Loch, L.P.N., Lehigh Family Practice Associates, LLC, and Leroy Hahn, 2016 Pa. Supeer LEXIS 2483 (Superior Court of Pennsylvania 2016).

DeLury v. Kretchner, 322 N.Y.S. 2d 517 (New York State Superior Court 1971).

Diana Retuerto v. Berea Moving Storage and Logistics, 38 N.E.3d 392 (Court of Appeals of Ohio 2015).

Doe v. B.P.S. Guard Services, Inc., 945 F. 2d 1422 (Eighth Circuit Court of Appeals 1991).

Dorris v. Abscher, 179 F.3d 420 (Sixth Circuit Court of Appeals 1999).

Electronic Communications Privacy Act of 1986, 18 United States Code, Sections 2510-2522.

Elgin v. St. Louis Coca Cola Bottling Co., 2005 U.S. District LEXIS 28976 (District Court for the Eastern District of Missouri 2005).

Ellenberg v. Pinkerton's, Inc. 202 S.E. 2d 701 (Georgia Court of Appeals 1973).

Emily Billing v. Martha's Vineyard Public Charter School, 2014 U.S. Dist. LEXIS 2438 (District Court for the District of Massachusetts).

French v. United Parcel Service, 2 F. Supp. 2d 128 (District Court for the District of Massachusetts 1998).

Forsberg v. Housing Authority of Miami Beach, 455 So.2d 373 (Florida Supreme Court 1984).

Fraser v. Nationwide Mutual Insurance Company, 352 F.3d 107 (Third Circuit Court of Appeals 2004).

Fry v. IBP, Inc., 15 F. Supp. 2d 1032 (District Court for the District of Kansas 1998).

George H. Larson v. United Natural Foods West Inc., 2014 Ariz. App. LEXIS 180 (Arizona Court of Appeals 2014).

Gilmore v. Enogex, Inc., 878 P.2d 360 (Oklahoma Supreme Court 1994).

Gracey v. Eaker, 747 So.2d 475 (Florida District Court of Appeal 1999).

Green, Michael Z. (Fall, 2001). A 2001 Employment Law Odyssey: The Invasion of Privacy Tort Takes Flight in the Florida Workplace. *Florida Coastal Law Journal*, Vol. 3, pp. 1-21.

Greenberg v. Alta Healthcare System, LLC, 2004 Cal. App. LEXIS 840 (California Court of Appeals 2004).

Howard, Christine E. (Spring, 2008). Emerging Technology and Employee Privacy: Symposium: Invasion of Privacy Liability in the Electronic Workplace: A Lawyer's Perspective. *Hofstra Labor & Employment Law Journal*, Vol. 25, pp. 511-523.

I.C.U. Investigations, Inc. v. Jones, 780 So. 2d 685 (Alabama Supreme Court 2000).

Jane Doe v. Bernabei & Wachtel, PLLC, 116 A.3d 1262, (District of Columbia Court of Appeals 2015).

Jennifer Pawlaczyk v. Besser Credit Union, 2014 U.S. Dist. LEXIS 150027 (District Court for the Eastern District of Michigan 2014).

Jews for Jesus, Inc. v. Rapp, 997 So.2d 1098 (Florida Supreme Court 2008).

Keller, Pamela V. (June, 2013). Balancing Employer Business Interests and Employee Privacy Interests: A Survey of Kansas Intrusion on Seclusion Cases in the Employment Context. *The University of Kansas Law Review*, Vol. 61, pp. 983-1019.

Kelley v. Schlumberger Tech. Corp., 849 F. 2d 41(First Circuit Court of Appeals1988).

Keeton, W. Page, Dobbs, Dan B., Keeton, Robert E, and Owen, David G. (1984). *Prosser and Keeton on Torts* (Hornbook Series 5th Edition). West Publishing Company: St. Paul, Minnesota.

Khrennikov, Ilyn (June 27 – July 3, 2016). Now the Boss Can Monitor Your Phone. *Bloomberg Businessweek*, pp. 31-32.

K-Mart Corp. v. Trotti, 677 S.W.2d 632 (Texas Court of Appeals 1984).

Kush v. Lloyd, 616 So.2d 348 (Florida Supreme Court 1992).

Lankford v. City of Hobart, 27 F. 3d 477(Tenth Circuit Court of Appeals 1994).

Levi Wilson v. Scott Lamp, State of Iowa, Jessica Dorhout-Van Engen, and John Doe, 142 F. Supp.3d 793 (District Court for the Northern District of Iowa 2015).

Liberti v. Walt Disney World, 912 F. Supp. 1494 (District Court for the Middle District of Florida 1995).

Love v. Southern Bell Telephone & Telegraph Co., 263 So. 2d 460 (Louisiana Court of Appeals 1972).

Maremont v. Susan Fredman Designs Group, Ltd., 2011 U.S. Dist. LEXIS 140446 (District Court for the Northern District of Illinois 2011).

Markovitch v. Panther Valley School District, 2014 U.S. Dist. LEXIS 102172 (District Court for the Middle District of Pennsylvania 2014).

Marrs v. Marriot Corp., 830 F. Supp. 274 (District Court for the District of Maryland 1992)

McLaren v. Microsoft Corporation, 1999 U.S. LEXIS 4103 (Texas Court of Appeals 1999).

Mgrditchian, Greg (2015). Employment and Social Media Privacy: Employer Justifications for Access to "Private" Material. *Rutgers Computer and Technology Law Journal*, Vol. 41, pp. 108-33.

Michael Stancombe v. New Process Steel LP, 2016 U.S. App. LEXIS 10038 (Eleventh Circuit Court of Appeals 2016).

Miller v. Motorola, 560 N.E.2d 900 (Illinois Court of Appeals 1990).

Muick V. Glenayre Elecs., 280 F.3d 741 (Seventh Circuit Court of Appeals 2002).

Mujtaba, B.G. (2014). *Managerial skills and practices for global leadership*. Florida: ILEAD Academy.

Nichols, Donald H. (2001). Window Peeping in the Workplace: A Look into Employee Privacy in a Technological Era. *William Mitchell Law Review*, Vol. 27, pp. 1587-1608.

Noyce, Lindsay (2011). Private Ordering of Employee Privacy: Protecting Employees' Expectations of Privacy with Implied-In-Fact Contracts. *American University Labor & Employment Law Forum*, Vol. 1, pp. 27-65.

O'Connor v. Ortega, 480 U.S. 709 (U.S. Supreme Court 1987).

O'Gorman, Daniel P. (2006). Looking out for Your Employees: Employers' Surreptitious Physical Surveillance of Employees and the Tort of Invasion of Privacy. *Nebraska Law Review*, Vol. 85, pp. 212-283.

Ozer v. Borquez, 940 P.2d 371 (Colorado Supreme Court 1997).

Pietrylo v. Hillstone Restaurant Group, 2009 U.S. Dist. LEXIS 88702 (District Court for the District of New Jersey 2009).

Quon v. Arch Wireless Operating Company, 529 F.3d 892 (Ninth Circuit Court of Appeals 2008).

Resley v. Ritz-Carlton Hotel Co., 989 F. Supp. 1442 (District Court of Florida 1997).

Restatement (Second) of Torts, Section 652. American Law Institute (1977).

Robertson, Mark W. and Kanaga, Mark A. (April, 2008). Office Watch: Employers Who Monitor Computer Use Must Take Into Account Their Employees' Reasonable Expectations of Privacy. *Los Angeles Lawyer*, Vol. 31, pp. 29-33.

Salazar v. Golden State Warriors, 124 F. Supp. 2d 1155 (District Court for the Northern District of California 2000).

Saldana v. Kelsey-Hayes Co., 443 N.W. 2d 382 (Michigan Court of Appeals 1989).

Sandra Gaynor c. American Association of Nurse Anesthetists and Brent Sommers, 2015 Ill. App. LEXIS 2969 (Illinois Court of Appeals 2015).

Schoening, Kelly and Kleisinger, Kelli (2010). Off-Duty Privacy: How Far Can Employers Go? *Northern Kentucky Law Review*, Vol. 37, pp. 287-321.

Sharon Diane Waltz v. Jonathan Wade Dunning, 2014 U.S. Dist. LEXIS 178660 (District Court for the Northern District of Alabama 2015)

Smyth v. Pillsbury Co., 914 F. Supp. 97 (District Court for the Eastern District of Pennsylvania 1996).

Souder v. Pendleton Detectives, Inc., 88 So. 2d 716 (Louisiana Court of Appeals 1952).

Sprague, Robert (Spring, 2008). Emerging Technology and Employee Privacy: Symposium: Rethinking Information Privacy in an Age of Online Transparency. *Hofstra Labor & Employment Law Journal*, Vol. 25, pp. 395-417.

Sprague, Robert (Fall, 2008). Orwell Was An Optimist: The Evolution of Privacy in the United States and Its De-Evolution for American Employees. *The John Marshall Law Review*, Vol. 42, pp. 83-184.

State Farm Fire & Casualty Co. v. Compupay, 654 So.2d 944 (Florida District Court of Appeal 1995).

Stockett v. Tolin, 791 F. Supp. 1536 (District Court of Florida 1992).

Sunbelt Rentals, Inc. v. Santiago Victor, 43 F. Supp.3d 1026 (District Court for the Northern District of California 2014).

Texas Health Resources, Trumble Insurance Company, and Texas Health Presbyterian Hospital Dallas v. Nina Pham, 2016 Tex. App. LEXIS 8336 (Court of Appeals of Texas 2016).

Thompson v. Johnson County Community College, 930 F. Supp. 501 (District Court for the District of Kansas 1996).

Thomas v. General Electric Co., 207 F. Supp. 792 (District Court for the Western District of Kentucky 1962).

Topolski v. Chris Leef General Agency, 2012 U.S. Dist. LEXIS 38691 (District Court for the District of Kansas 2012).

Vernars v. Young, 539 F.2d 966 (Third Circuit Court of Appeals 1976).

Vernon v. Medical Management Associates of Margate, Inc., 912 F. Supp. 1549 (District Court for the Southern District of Florida 1996).

Watkins v. L.M. Berry Co., 704 F.2d 577 (Eleventh Circuit Court of Appeals 1983).

Wesche, Todd M. (2002). Reading Your Every Keystroke: Protecting Employee E-mail Privacy. *Journal of High Technology Law*, Vol. 1, pp. 101-119.

Author Biographies

Frank J. Cavico is a Professor of Business Law and Ethics at the H. Wayne Huizenga School of Business and Entrepreneurship of Nova Southeastern University in Ft. Lauderdale, Florida. He has served as a faculty member at the school for 30 years. He is a member of the Management Department. He teaches business law and business ethics classes primarily at the graduate level in the MBA program; and Professor Cavico also teaches in the MPA program where he teaches the required Administrative Law and Ethics course. He also teaches the undergraduate business law course. He is the professor who brought ethics into the graduate business school by means of a course called "Management Ethics." He is the creator of current law and ethics course "The Legal, Ethical, and Social Values of Business," which is a required core course; and he presently serves as course leader for that course as well as an undergraduate business law course. He has also taught Constitutional and Administrative Law at the doctoral level in the Huizenga School. He has been the recipient of the Professor of the Year and Faculty of the Year Awards at the Huizenga School; and he was a nominee for the Professor of the Year Award for the university. He is the author of several books and numerous law review and management journal articles. Professor Cavico holds an LL.M degree from the University of San Diego, a J.D. from St. Mary's University, a Master's degree in Political Science from Drew University, and a B.A. in Political Science from Gettysburg College.

Bahaudin G. Mujtaba is a Professor of International Management at the Huizenga College of Business and Entrepreneurship of Nova Southeastern University. Bahaudin is the author and coauthor of books dealing with diversity, ethics and business management. During the past thirty years he has had the pleasure of working with managers and human resource professionals in the United States, Brazil, India, Afghanistan, Pakistan, St. Lucia, Grenada, Vietnam, Malaysia, Thailand, Bahamas, and Jamaica. This diverse exposure has provided him many great insights in management from the perspectives of different firms, people groups, and countries.