**SEAL AND INSULATE: PROTECTING PRIVACY IN THE WORKPLACE**

**TABLE OF CONTENTS**

**Page**

[I. INTRODUCTION 1](#_Toc446593890)

[II. LAWS PROTECTING EMPLOYEE PRIVACY 1](#_Toc446593891)

[A. Employee Polygraph Protection Act (“EPPA”) 1](#_Toc446593892)

[B. National Labor Relations Act (“NLRA”) 4](#_Toc446593893)

[C. Fair Credit Reporting Act (“FCRA”) 6](#_Toc446593894)

[D. Wiretapping 8](#_Toc446593895)

[E. Medical Records 12](#_Toc446593896)

[F. Employee Drug Testing-Privacy Under Current Drug Testing Laws 15](#_Toc446593897)

[G. Constitutional Right of Privacy 17](#_Toc446593898)

[H. Common Law Torts 19](#_Toc446593899)

[I. Laws Protecting Applicant and/or Employee Social Media 20](#_Toc446593900)

[III. PROTECTING THE PRIVACY OF EMPLOYERS 21](#_Toc446593901)

[A. Criminal Trade Secrets Provision 21](#_Toc446593902)

[B. The Florida Computer Crimes Act 22](#_Toc446593903)

[C. Common Law Conversion 23](#_Toc446593904)

[D. Duty of Loyalty 23](#_Toc446593905)

[F. Restrictive Covenants 25](#_Toc446593906)

[G. Reasonable Employer Actions to Retain Information Secrecy 31](#_Toc446593907)

[IV. CONCLUSION 34](#_Toc446593908)

[APPENDIX A 35](#_Toc446593909)

**SEAL AND INSULATE: PROTECTING PRIVACY IN THE WORKPLACE**

**I. INTRODUCTION**

Employers must be cognizant of the parameters of their employees’ rights to privacy, lest they unwittingly violate those rights and find themselves entangled in litigation. Today’s technology enables employers to monitor their employees like never before. Virtually everything that employees do on an employer’s telephone system or computer system can be monitored. Moreover, employers have access to confidential information about employees that is not generally known to the public. This session will address employee privacy concerns, and what employers can and cannot do when it comes to employee privacy.

Similarly, employers have rights to privacy. An employer’s customers, employees, and confidential business information are its most valuable assets. Yet, each of those assets is susceptible to threats. One such threat stems from employees who depart to work for a competing business and take with them customer lists, distributor lists, and other proprietary information, or who capitalize upon their relationships with customers and co-workers by trying to take them away. Fortunately, there are laws that protect the privacy interests of employers, and there are steps that employers can take to protect themselves from employees who would violate those interests.

**II. LAWS PROTECTING EMPLOYEE PRIVACY**

**A. Employee Polygraph Protection Act (“EPPA”)**

 *1. General Protections*

 In 1988, the EPPA was passed and, for the most part, ended the use of polygraphs or lie detectors in the private sector pre-employment or employment setting. Private employers are prohibited from requiring, suggesting, or causing applicants or employees to take a polygraph or lie detector test. In fact, merely asking an employee to take a lie detector test violates the law, even if the lie detector test is never given and no adverse employment action is taken. In addition, employers may not use, accept, refer, inquire or take adverse actions as a result of a third party administering a polygraph or lie detector test. Retaliation against an individual for exercising his/her rights provided by the EPPA is also illegal. The EPPA has a notice posting requirement. The EPPA does not preempt state or local laws or collective bargaining agreements that provide more protections to employees than the EPPA.

 *2. Exemptions*

 The EPPA has several exemptions. For example, there is the exemption for federal, state and local governments as mentioned above. There is also an exemption for pre-employment testing of employees of security service firms (armored car, alarm and guard), and of pharmaceutical manufacturers, distributors and dispensers of controlled substances. In addition, there is an exemption when an employer is investigating a theft or a series of thefts. Nonetheless, strict rules apply and must be followed or the exemption will be lost. More specifically:

 1) The lie detector test must be administered in connection with an ongoing investigation involving economic loss or injury to the employer’s business such as theft, embezzlement, misappropriation or an industrial espionage or sabotage;

 2) The employee had to have access to the property that is the subject property of the investigation;

 3) The employer must have a reasonable suspicion that the employee was involved in the incident or activity;

 4) The employer must execute a statement provided to the employee before the lie detector test that:

a) Sets forth with particularity the specific incident or activity being investigated and the bases for testing particular employees;

b) Is signed by a person… authorized to legally bind the employer;

c) Is retained by the employer for at least three (3) years; and

d) Contains at a minimum:

 i. an identification of the specific economic loss or injury to the business of the employer;

 ii. a statement indicating that the employee had access to the property that is the subject of the investigation; and

 iii. a statement describing the basis of the employer’s reasonable suspicion that the employee was involved in the incident or activity under investigation. 29 U.S.C. §2006(d).

Additionally, lie detector test results may not be used against the employee unless the employer has additional evidence to conclude adverse employment action is appropriate. 29 U.S.C. §2007(a)(1). There are additional procedural rules that must be strictly adhered to when a lie detector test is to be given and before any adverse employment action is taken. Failure to strictly adhere to these rules will result in loss of the exemption. The results of a lie detector test are confidential and may not be disclosed by the employer, except to a governmental agency if the “disclosed information is an admission of criminal conduct.” 29 U.S.C. §§2008(c)(1) and (2).

 *3. Remedies*

 Individuals asserting a violation of the EPPA have a private cause of action. They must only prove that the result of a lie detector test was one factor leading to an adverse employment action, not the sole factor. *Worden v. SunTrust Banks, Inc.* Violations may result in legal or equitable relief, including employment, reinstatement, promotion, lost wages, benefits, attorney’s fees and costs. At least one court has held that damages for emotional distress are recoverable. In addition, another court has suggested that under the right circumstances punitive damages may be recoverable as well.

 *4. Florida Case Law Ends Use of Polygraphs for Public Employees*

 The EPPA effectively ended the use of polygraphs only for private employers, but not for public employees. However, in Florida, approximately five (5) years before the passage of the EPPA, the Florida Supreme Court effectively ended the public sector employers’ use of polygraph. In *Farmer v. City of Fort Lauderdale*, the Court held that polygraph evidence was not sufficiently reliable to support the termination of a public employee. Further, the Court provided that a public employee had the right to refuse to incriminate himself, in order to maintain his employment. Thus, for practical purposes, this case ended the use of polygraphs to support termination decisions of Florida public employees.

**B. National Labor Relations Act (“NLRA”)**

*1. Concerted Activity*

 Section 7 of the NLRA provides unorganized, private employees with the right to engage in protected concerted activity. More specifically, the NLRA gives employees the right to act together to try to improve their pay, benefits, working conditions, and other terms and conditions of employment, even without a union. Such group activity is referred to as concerted activity. The NLRA prohibits employers from restraining or interfering with this right. If an employee suffers an adverse employment action for taking part in protected concerted activity, the NLRA provides a means to remedy the wrong and making the employee whole. These NLRA protections do not extend to managers and supervisors.

 *2. Confidentiality Policies*

 An employer who interferes with or restrains employees’ Section 7 rights, violates Section 8 of the NLRA. Policies can restrain these rights, thereby violating the NLRA, if the policies prohibit employees from discussing their compensation information, sharing employee personal information, benefits and other terms and conditions of employment. The NLRB more recently has also determined that general policies that do not specifically mention compensation or other terms or conditions of employment can also violate Section 7 rights.

 In the case of *Flex Frac Logistics, LLC,* the NLRB determined an employer’s at will agreement was overly broad and ambiguous and prohibited, or may reasonably be read to prohibit employees from discussing wages or other terms and conditions of employment, and thus, violated the NLRA. The agreement’s confidentiality provision stated:

 Confidential Information

 Employees deal with and have access to information that must stay within the Organization. Confidential Information includes, but is not limited to, information that is related to: our customers, suppliers, distributors; Silver Eagle Logistics LLC, organization management and marketing processes, plans and ideas, processes and plans, our financial information, including costs, prices; current and future business plans, our computer and software systems and processes; personnel information and documents, and our logos, and art work. No employee is permitted to share this Confidential Information outside the organization, or to remove or make copies of any Silver Eagle Logistics LLC records, reports or documents in any form, without prior management approval. Disclosure of Confidential Information could lead to termination, as well as other possible legal action.

 The NLRB opined that an employer “violated Section 8(a)(1) of the Act when it maintained a work rule that reasonably tended to chill employees in exercise of their Section 7 rights.” According to the NLRB, the trouble with the at-will agreement was that it generally defined “Confidentiality Information” to include “personnel information and documents” to persons “outside the organization” which “necessarily include[d] wages and therefore reinforced the likely inference that the rule proscribe[d] wage discussion with outsiders” (or union organizers). The Court of Appeals affirmed the decision.

 The NLRB has even gone so far with this theory as to find violations of Section 7 rights, even when no employee suffered an adverse employment action and there was no evidence of enforcing the violative policy language. In the case of *Quicken Loans, Inc.,* the NLRB found Quicken’s employment agreement contained language violating Section 7 rights. The offending language was found in a confidentiality provision that prohibited disclosure of information and a non-disparagement provision.[[1]](#footnote-1) The Board again stated that the proper inquiry was whether the agreement language was likely to chill employees’ Section 7 rights. The NLRB specifically held that the confidentiality provision language effectively prohibited employees from discussing their wages, benefits, addresses or telephone numbers of other employees, with union representatives and each other, thereby violating the NLRA Section 7 rights. Further, the non-disparagement provision inhibited employees’ exercise of their concerted activity rights to criticize their employer and its products within limits.

 In conclusion, audit your handbook policies closely. When developing confidentiality policies, non-disclosure, and other general policies, make sure the language used in such policies cannot be “reasonably understood by employees to restrict discussion of their wages, benefits and other terms and conditions of employment” or sharing co-worker’s names or contact information with each other or a labor organization. Language prohibiting employees from disclosing personnel information, as well as employee contact information with each other and outsiders will likely offend employees’ right to exercise their concerted activity rights.

**C. Fair Credit Reporting Act (“FCRA”)**

 *1. Generally*

 Congress passed the FCRA to protect individuals against the use of consumer reports without their knowledge and without opportunity to correct erroneous or misleading information. Congress saw a “need to insure that consumer reporting agencies exercised their grave responsibilities with fairness, impartiality, and with a respect for the consumer’s “right to privacy.” 15 U.S.C. §1681(a)(4). The law also gives consumers an opportunity to correct erroneous information found in credit reports. A consumer report is defined as:

Any written, oral or other communication, of any information by a consumer reporting agency bearing on the consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used, or collected in whole or in part, for the purpose of serving as a factor in establishing the consumer’s eligibility for...employment purposes….[[2]](#footnote-2)

The term “employment purposes” is defined as ….. a consumer report used for evaluating a consumer for “employment, promotion, reassignment, or retention as an employee”. 15 U.S.C. §1681a(h). Importantly, the FCRA applies only to reports secured by consumer reporting agencies (“CRA”). A CRA is defined as “any person which, for monetary fees, dues or on a cooperative nonprofit basis, regularly engages in whole or in part, in the practice of assembling or evaluating consumer credit information, or other information on consumers for the purpose of furnishing consumer reports to third parties and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. 15 U.S.C. §1681a(f).

 *2. Privacy Protections*

 To use consumer reports, employers must certify proper use and compliance with the FCRA disclosure and authorization provisions. Before taking any adverse employment action in part or fully because of a credit report, the employer must provide a copy of the report and a summary of rights as specified by the FTA to the consumer. Only after a reasonable time has passed, may the employer proceed with the desired adverse employment action.

 Additionally, the Fair and Accurate Credit Transaction Act (“FACTA”), amended the FCRA to help prevent identity theft. FACTA requires consumer reporting agencies to properly dispose of consumer information while protecting against unauthorized disclosure or use of the information collected and disposed of. 16 CFR §682.3. Further, any business that uses consumer reporting must adopt reasonable measures and procedures to properly dispose of consumer reports to protect against unauthorized access to and use of information in connection with its disposal. Reasonable measures include implementing policies and procedures that require burning, pulverizing, or shredding paper containing consumer information to ensure that it cannot be read or reconstructed. This can be accomplished by hiring a disposal vendor or by using a shredder. FACTA also requires the proper disposal of devices and/or mediums used to store such consumer information.

 The FCRA provides consumers with a private right of action for violation of the FCRA. Willful violations can result in the greater of actual damages or up to $1,000, emotional distress, and loss of reputation, punitive damages, attorney fees and costs. Negligent violations are also actionable and may result in actual damages, attorney’s fees and costs.

**D. Wiretapping**

 *1. Chapter 934, Florida Statutes*

 Florida Statutes make it a crime to record conversations without the knowledge and consent of those conversing. For an oral communication to be protected, the speaker must have an actual subjective expectation of privacy, along with a societal recognition that the expectation is reasonable. Therefore, listening to a private conversation on a phone extension without all parties’ knowledge and consent would violate the law.

 *2. Federal Electronic Communications Privacy Act (“ECPA”)*

 The ECPA is a federal statute that created a private cause of action for the intentional interception of electronic communication and against those who gain unauthorized access to stored electronic communication. ECPA’s explicit intent is to protect electronic communication including data shared by computer. There are two parts of the Act that are relevant to employer/employee relationships. Title I is commonly referred to as the Wiretap Act and prohibits intentional interception of electronic communication. Title II is commonly referred to as the Stored Communication Act (“SCA”) and prohibits unauthorized access to shared electronic communication.

 The Wiretap Act prohibits the interception of electronic communication. Interception means “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” Content when used with respect to oral or electronic communication “[includes] any information concerning the substance, purport, or meaning of that communication.” The term “content” has been generally understood to exclude information such as to whom or from whom an electronic communication is being sent and also information such as that contained in the subject line of an email message. The Act contains both criminal and civil penalties. The Act does not protect employees from monitoring by GPS or silent video. Listening to a personal phone conversation is inappropriate once an employer determines the call is personal.

 Two open issues under the Wiretap Act include whether or not an interception is also an acquisition of stored communication, and whether or not the acquisition must be contemporaneous with transmission. Several courts have interpreted “intercept to exclude stored communications.” The majority view holds that employers can access email, unless the emails are intercepted in transit and not stored, assuming the employer has its own internet service. These cases rely primarily on the interpretation that the ECPA is divided into separate Title I on interception and II on storage. To violate Title I, the intercept must occur contemporaneously with transmission.

 *3. Exceptions*

 Two exceptions to coverage, the consent and provider exceptions, have been interpreted by courts to provide a level of protection to employers that permit them to monitor email content in approved circumstances.

 a. The consent exception. To come within the ambit of the consent exception, one party to electronic communication must give consent to intercept the communication prior to its interceptions. The consent exception provides:

 It shall not be unlawful under this this Chapter for a person not acting in the color of the law to intercept a wire, oral or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of criminal or tortious act in violation of the constitution or laws of the U.S. or any state.(Emphasis added). 18 U.S.C. §2511.

 The Second Circuit Court of Appeals has stated that the consent exception is to be broadly construed. The majority of courts have required consent “in fact”. Courts based this “consent” upon the factual circumstances presented in the cases. If the defendant can show that the employee or plaintiff knew of the particular complained of monitoring and the court determines the employee’s actions demonstrate that the employee or complaining individual gave approval, the court has found consent in fact exists. For example, courts have found implied consent is consent in fact where the plaintiff knew of the monitoring and continued to engage in monitored activity. Courts have held that implied consent was found based upon handbook policy providing for monitoring. Thus, for the most part, the consent exception applies where employers develop an electronic communication policy that provides that all electronic communications belong to the employer and will be monitored. By accepting employment, employees consent to the employer accessing all the employee’s communication on the employer’s system.

 Nevertheless, there are limits to the exception. In *Pietrylo v. Hillstone Rest. Grp.*, a jury verdict was upheld where an employee’s consent was determined to be coerced from the employee. Two employees developed a chat group on ‘My Space.com’ for criticizing and maligning the employer and management. Access was available to certain limited restaurant employees on an invitation and password provision basis only. An employee gave the managers access. However, she testified that she felt compelled to give her password and username or she would get in trouble. The managers continued to access the chat room – even after the employee made clear she had reservations to their accessing the site.

In the case of *Quon v. Arch Wireless Operating C*o.a police officer sued a third party provider when it gave the Ontario Police Department copies of his texts upon request. Although the City provided the public officer with beeper service, the third party provider was found to have violated the ECPA when it provided copies of the officer’s texts without the officer’s consent. The Court also determined that Officer Quon’s 4th Amendment Right to Privacy did not extend to the private third party provider.

 Other activity that has been found to amount to illegal interception includes: (i) use of software application to covertly intercept personal passwords to email accounts. The employer captured the employee’s keystrokes while in transit. This action constituted interception under the law *Brahmana v. Lembo*; and (ii) acquiring electronic communication from a transient storage location which was part of the communication process. *U.S. v. Councilman, 418 F.3d 67* (1st Cir. 2005).

 b. The Provider Exception. The SCA also has exceptions. One such exception that is valuable to employers and is called the Provider Exception:

“Exceptions: (c) Exceptions. - Subsection (a) of this Section does not apply with respect to conduct authorized - (1) by the person or entity providing a wire or electronic communications service;..” 18 U.S.C §2701.

This exception permits employers who have their own email system with servers for storage to access emails once the emails are stored on the employer’s servers. This exception does not apply, however, if the employer uses a third party provider such as Gmail or Hotmail as a source of its email communication. It also doesn’t apply where an employer accesses an employee’s personal email account.

 In one case, the employer was found to have violated the ECPA when it hacked into its former employee’s personal email account without authorization. The plaintiff employer was able to access defendant’s Hotmail account after he left his username and password information stored on plaintiff’s computers. One email account was accessed after the username and password fields automatically populated on the plaintiff’s computers. Another email account was accessed by plaintiff when plaintiff guessed the defendant’s password. The employer’s accessing the former employee’s private email accounts violated the ECPA, even where he left his username and password on the employer’s computer. *Pure Power Boot Camp v. Warrior Fitness Boot Camp.*

**E. Medical Records**

 *1. Americans With Disabilities Act (“ADA”)*

 The ADA requires that medical records be retained in a confidential manner. The basic rule, with limited exceptions, requires that employers keep confidential any medical information they learn about an applicant or employee. Medical information must be kept on separate forms in a separate locked confidential medical file and treated as a confidential medical record. Only specific HR persons should have access to the medical file on an as needed basis.

 Exceptions to these general rules include:

a) Supervisors and managers may be informed about necessary restrictions on the work or duties of the employees and necessary accommodation;

b) First aide and safety personnel may be informed if a disability might require emergency treatment or special procedures in case of fire or evacuation; and

c) Government officials investigating compliance with the ADA and other federal and state laws prohibiting discrimination on the basis of disability or handicap should be provided relevant information.

 However, employees and applicants currently engaging in the illegal use of drugs are not covered by the ADA when an employer acts on the basis of such use. Tests for illegal drugs are not subject to the ADA's restrictions on medical examinations. Nevertheless, other state statutes may make the test results and other information confidential, like §440.102, Florida Statutes. Additionally, where alcohol, and in some states, marijuana are legal drugs, tests results for these drugs may arguably have to be maintained confidentially under the ADA.

 Once an individual becomes an employee, employers may ask only disability related questions or require medical examinations that are job related and consistent with business necessity. This means that an employer can obtain medical information when it reasonably believes that an employee is unable to perform essential job functions or creates a direct threat as a result of his condition. Only limited information may be sought to determine if the employee is entitled to a requested accommodation.

If an employee requests reasonable accommodation and the need for accommodation is not obvious, the employer may require reasonable documentation of the employee's entitlement to reasonable accommodation. While the employer may require documentation showing that the employee has a covered disability and stating his functional limitations, it is not entitled to medical records that are unnecessary to the request for reasonable accommodation. The employer may need to ask questions concerning the nature of the disability and the individual's functional limitations in order to identify an effective accommodation. While the individual with a disability does not have to be able to specify the precise accommodation, he does need to describe the problems posed by the workplace barrier.

Information can be confidential even if it contains no medical diagnosis or treatment course and even if it is not generated by a health care professional. For example, an employee's request for a reasonable accommodation would be considered medical information subject to the ADA's confidentiality requirements.

 The employer is not permitted to disclose to a complaining co-worker that an employee has a disability and is being reasonably accommodated. The EEOC advises employers to tell a complaining employee that the matter involves a matter of co-worker’s privacy and that the employer treats such matters confidentially. The complainer should be encouraged to understand that if he had a similar situation, the matter would be treated confidentially as well.

 *2. The Genetic Information Nondiscrimination Act of 2008 (“GINA”)*

 With limited exceptions, GINA prohibits employers from requesting, requiring, or purchasing genetic information about applicants, employees, or their families. Employers should ensure that if they request medical records or a medical exam that only the limited medical information needed that is job related and consistent with business necessity, is obtained. To ensure compliance with GINA, employers should include the GINA safe harbor language on any medical release and/or medical examiners form requesting only job related medical information. The safe harbor language is found in 29 C.F.R. §1635.8(b)(1)(i)(B). Should an employer secure genetic information, this information should be confidentially maintained in the employee’s medical file.

 *3. Florida HIV Protections, §760.50, Florida Statutes*

 Florida has a statute protecting those with HIV or perceived as having HIV from discrimination. The statute prohibits any person from requiring an individual to take a human immunodeficiency virus related test as a condition of hiring, promotion, or continued employment, unless the absence of human immunodeficiency virus infection is a bona fide occupational qualification for the job (BFOQ). Every employer who provides or administers health insurance benefits or life insurance benefits, to its employees must maintain information relating to the medical condition or status of any person covered by such insurance benefits confidentially. Florida Statute §760.50 creates an individual cause of action in the circuit court for violation of the statute. An individual may recover for an employer’s failure to maintain the required confidentiality, for each violation. Recovery may include:

a. Liquidated damages of $1,000 or actual damages, whichever is greater.

b. For intentional or reckless violation of a provision of this Section - liquidated damages of $5,000 or actual damages, whichever is greater.

c. Reasonable attorney’s fees.

d. Injunctive relief, as the court may deem appropriate.

**F. Employee Drug Testing-Privacy Under Current Drug Testing Laws**

 *1. Department of Transportation Drug Testing*

 Employers participating in the DOT drug or alcohol testing process are prohibited from releasing individual test results or medical information about the employee or applicant to third parties without the employee’s specific written consent. Third parties include potential employers. “Specific written consent” means a statement signed by the employee that he agrees to the release of a particular piece of information to a particular, explicitly identified person or organization at a particular time. “Blanket releases,” specifying for example that the employee agrees to release all test results, do not satisfy the requirement. Further, a specific release of information to a category of parties is likewise prohibited.

 On December 22, 2015, DOT issued a new driver disclosure and authorization form. The form is to be used by all employer account holders of the Pre-employment Screening Program (“PEP”). The form must be a stand-alone document and may not be combined with any other language and must contain the signature, date, and the date of signature. The form must be maintained for three (3) years whether or not the driver is hired. This form is attached hereto as Appendix A.

 *2. Florida’s Worker’s Compensation Drug Testing*

 An employee must be able to confidentially report to a medical review officer the use of prescription or nonprescription medications both before and after being tested. Any and all explanation and/or challenge of the positive test result, a written explanation as to why the employee’s or job applicant’s explanation is unsatisfactory, along with the report of positive result, must be kept confidential by the employer pursuant to the statutory confidentiality provision and must be retained by the employer for at least 1 year.

 If drug testing is conducted based on reasonable suspicion, the employer must also promptly detail in writing the circumstances which formed the basis of the determination that reasonable suspicion existed to warrant the testing. The original documentation must be kept confidential by the employer and shall be retained by the employer for at least 1 year.

 All information, interviews, reports, statements, memoranda, and drug test results, written or otherwise, received or produced as a result of a drug-testing program are confidential and exempt from the provisions of Public Records Law and §24(a), Article I of the State Constitution, and may not be used or received in evidence, obtained in discovery, or disclosed in any public or private proceedings, except in accordance with §440.102, Florida Statutes, or in determining compensability under worker’s compensation.

 Employers, laboratories, medical review officers, employee assistance programs, drug rehabilitation programs, and their agents may not release any information concerning drug test results obtained without a written consent form signed voluntarily by the person tested, unless such release is compelled by an administrative law judge, a hearing officer, or a court of competent jurisdiction pursuant to an appeal taken under this Section or as deemed appropriate by a professional or occupational licensing board in a related disciplinary proceeding. The consent form must contain, at a minimum:

 1. The name of the person who is authorized to obtain the information.

 2. The purpose of the disclosure.

 3. The precise information to be disclosed.

 4. The duration of the consent.

 5. The signature of the person authorizing release of the information.

 Information on drug test results may not be used in any criminal proceeding against the employee or job applicant. Information released contrary to this Section is inadmissible as evidence in any such criminal proceeding. Notwithstanding the confidentiality requirement of the statute, an employer, agent of an employer, or laboratory conducting a drug test is not prohibited from having access to employee drug test information or using such information when consulting with legal counsel in connection with actions brought under or related to this Section or when the information is relevant to its defense in a civil or administrative matter.

**G. Constitutional Right of Privacy**

 The origins of an individual’s right to privacy is found in the Fourth Amendment to the United States Constitution. Nevertheless, the Fourth Amendment only protects against governmental search and seizure, thereby, protecting for the most part public employees. It has no power to affect private employers’ searches, unless the private employer violates an employee’s Fourth Amendment rights by performing a search for, with, or at the request of law enforcement. Thus, to prevent such claims, private employers should not involve law enforcement in its search without a warrant.

 Additionally, employers should have a policy specifying what locations and non-personal items, the employer may want or need to search like offices, lockers, computers, desks, file cabinets and emails, thereby eliminating employees’ reasonable expectation of privacy in such items.

 The seminal federal case regarding whether a public employee had a constitutional right to privacy in his workspaces is *O’Connor v. Ortega*. The federal employee brought an action for breach of his right to privacy in his desk, file cabinet, and office after his employer examined and removed some of his personal items from the searched locations. The U.S. Supreme Court found that the employee had an expectation of privacy in his desk, and file cabinet because he did not share the items and used them to store his personal items. Importantly, the employer did not have a policy providing that employees had no expectation of privacy in the searched locations.

 In *O’Connor*, Justice O’Connor’s plurality determined the proper test for whether a search violated a public employee’s 4th Amendment right to privacy was the operational realities test. 1) This test requires consideration of the operational realities of the workplace to determine if the employee’s 4th Amendment right are implicated (i.e. whether he would have an expectation of privacy) and 2) Where an employee has a legitimate privacy expectation and the employer’s intrusion is the result of a non-investigatory work-related purpose or for investigation of a work-related misconduct, whether the search is reasonable under the circumstances. Under this test, a warrantless search is reasonable if it is justified at its inception and if measures adopted are reasonably related to the objectives of the search and not excessive in light of the circumstances giving rise to the search.

 In *Quon* *supra*, the Court assumed the employee had a right to privacy in his texts messages found on his work-issued beeper in absence of a policy to the contrary. However, the court failed to explicitly hold that public employees have a reasonable expectation of privacy in electronic communication on employers issued devices. The Court also observed that the jury determined the police chief ordered the search in order to determine whether the character limit on texts per month was sufficient to meet the City’s needs. Using the operational realties test, the Court, determined this was a legitimate work-related rationale requiring only a reasonable standard for the search. The scope of the search, reading the transcript of Officer Quon’s texts over two (2) months was also found to be reasonable. It was an efficient and expedient means of determining whether Officer Quon’s overages were work-related or not. Therefore, the search as not found to be excessively intrusive and did not violate Officer Quon’s 4th Amendment rights.

**H. Common Law Torts**

 *1. Invasion of Privacy*

Causes of action for invasion of privacy have been brought in 3 contexts:

a. Misappropriation of a person’s name or likeness for another’s benefit.

b. Intrusion – physically or electronically into one’s personal space or quarters.

c. Public disclosure of private facts.

Our focus is on the second context, intrusion physically or electronically into one’s personal space or seclusion. Such claims arise in the context of searching an office, locker, computer, email, social media site, or other work space. However, the degree of intrusion required to prove such a tort action must cause outrage, mental suffering, shame or humiliation to a person of ordinary sensibilities. A number of courts have determined search of an employee’s desk, office and/or computer not to be actionable. Key in these decisions is the extent to which the employee possessed reasonable expectations of privacy in these work spaces. The more actions an employer takes to communicate an absence of privacy in various work venues, the more likely legal attacks on the employer searches will fail. Employers diminish expectation of privacy by posting company privacy policy, discussing privacy policies in staff meetings, publishing privacy policies in the company handbooks, and attaching the privacy policy upon entering the company’s internal data network.

 In summary, to avoid common law breach of privacy tort action, employers should have a privacy policy that clearly gives the employer the right to access workplace spaces. The policy should make clear that the employees have no expectation of privacy in offices, desk, files, computers, emails, data files, and any other workplace space the employer sees as its property and/or it may want or need to access. Employers should drive this point home by ensuring they have current computer and email passwords, prescribe what category of documents may be password protected, and ensure it has keys to all locked spaces.

**I. Laws Protecting Applicant and/or Employee Social Media**

 It is extremely common for employers to check social media like LinkedIn or Facebook when vetting candidates for employment. LinkedIn shows users those who have recently viewed a user’s profiles, unless the vetting user pays for an upgrade version, blocking this information.

Public Facebook pages potentially contain pictures of the individual and may also show or depict protected life style choices. It’s fair to say that most human resources professionals know that by looking at such social media sites they increase the odds that their employer may be sued for discrimination. Pictures of the candidates often indicate the race, gender, and/or off-duty activities of the individual. As a result, companies may be wise to develop policies prohibiting or restraining management’s use of such social media sites for hiring or promotional purposes.

 Stories of managers requiring applicants and/or employees to access the individuals’ social media sites during the application process or after employment (and discipline in some cases) have prompted states to pass laws regarding employers use and access of social media.[[3]](#footnote-3) Many states have statutes protecting employees and/or applicants, from having to provide usernames and passwords to employers to access the individual’s personal social media accounts.[[4]](#footnote-4) Some of these laws also protect employees and/or applicants from employer requests to change privacy settings, to “shoulder surfing”, to add the employer or potential employer to his/her contact list, and/or from retaliation. It is also not unusual for these statutes to permit access to social media accounts opened for the employer and/or where the employer is investigating employee misconduct or theft of proprietary assets or information.

To understand each state’s statute, it must be closely examined for its particular proscriptions and prescriptions. Florida presently has no such law. Be wise; prohibit your managers from asking applicants and employees to access their applicant’s and/or employees’ social media pages unless the potential benefit/need significantly outweighs the potential harm.

**III. PROTECTING THE PRIVACY OF EMPLOYERS**

 **A. Criminal Trade Secrets Provision**

 Employers can use §812.081 of the Florida Statutes to their benefit when addressing the inappropriate use of a trade secret. This Section makes it a felony to steal or misappropriate a trade secret. Under this Section, a trade secret is defined as:

[T]he whole or any portion or phrase of any formula, pattern, device, combination of devices, or compilation of information which is for use, or is used, in the operation of a business and which provides the business an advantage, or an opportunity to obtain an advantage, over those who do not know or use it [and] includes any scientific, technical, or commercial information, including any design, process, procedure, list of suppliers, list of customers, business code, or improvement thereof.

 Nevertheless, it is vital that employers take measures to protect the privacy of their trade secrets, or else they may lose their status as trade “secrets” that are subject to protection. Thus, unless there is evidence that proper security measures have been undertaken, otherwise protectable information may not qualify as a trade secret. For example, in *Cubic Transp. Systems, Inc. v. Miami-Dade County*, a court found that documents a company submitted to the County were subject to the Public Records Law because the company failed to take reasonable efforts to maintain the secrecy of the documents. Although the company claimed that the documents contained trade secrets, they failed to mark the documents confidential and did not assert a timely claim of confidentiality. Since the issue of secrecy is a question of fact and will be determined based upon the circumstances of each case, employers are well-advised to take prompt reasonable security measures to ensure that confidential information which they believe constitutes a trade secret, as defined by the Statute, is designated as such. In addition to the substantive steps identified below, an employer can also protect itself by marking the information “confidential” and limiting access to the information to only a few key employees.

 **B. The Florida Computer Crimes Act**

Florida law also provides criminal penalties for the unauthorized use and disclosure of certain trade secrets relating specifically to computer networks. Under §815.04 of the Florida Statutes, it is a crime to modify, destroy, disclose, or take any computer data, programs, or supporting documentation without prior authorization. A violation of this Statute constitutes a felony of the third degree. Section 815.05 of the Florida Statutes further provides that it is a misdemeanor of the first degree to modify, destroy, take, injure or damage equipment or supplies used or intended to be used in a computer system or computer network.

**C. Common Law Conversion**

 Employees who steal an employer’s confidential business information may be held liable for “conversion.” Conversion is an act of dominion wrongfully asserted over another’s property. In essence, conversion is an unauthorized act that deprives another of his property permanently or for an indefinite time. In *Warshall v. Price,* for example, a physician claimed that another physician wrongfully used a patient list without consent for the purpose of soliciting patients on the list. The physician who was being sued argued that he only took a copy of the list. Therefore, the list copying physician argued the physician who was suing was never deprived of the list. On appeal, the Court held that it was not necessary for a person to deprive another of exclusive possession of his property in order to be liable for conversion. Therefore, the physician who was being sued for conversion could be held liable, even though he took only a copy of the list.

 **D. Duty of Loyalty**

 Florida law recognizes the tort of breach of a duty of loyalty in an employment setting. The general rule with regard to an employee’s duty of loyalty to his employer is that an employee does not violate his duty of loyalty when he or she merely organizes a corporation during his employment to carry on a rival business after the expiration of his employment. However, that employee may not engage in disloyal acts in anticipation of his future competition, such as using confidential information acquired during the course of his employment or soliciting customers and other employees prior to the end of his employment.

 **E. Uniform Trade Secrets Act (“UTSA”)**

The UTSA, which has been adopted by Florida and numerous other states, prohibits employees and other individuals from misappropriating or threatening to misappropriate, trade secrets. Under the Act, a trade secret is defined as information, including a formula, pattern, compilation, program, device, method, technique, or process that: (a) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means, by other persons who can obtain economic value from its disclosure or use; and (b) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Factors used to determine whether information is a trade secret include: (1) the extent to which the information is known outside of the employer’s business; (2) the extent to which the information is known by employees and others involved in the business; (3) the extent of measures taken by the employer to guard the secrecy of the information; (4) the value of the information to the employer and to competitors; (5) the amount of effort or money expended by the company in developing the information; and (6) the extent to which the information could be easily or readily obtained through an independent source. Examples of trade secrets may include existing and potential customer lists, unless they are readily ascertainable by the general public. *See* *Unistar v. Child* (where the creation of a customer list required considerable effort, knowledge, time and expense, it qualifies as a trade secret and cannot be used by former employees for their own benefit); *Templeton v. Creative Loafing* (where no great expertise was needed to gain magazine distribution information, a former employee could not be precluded from utilizing contacts gained during employment); and *Sethscot Collection Inc., v. Drbul* (where “prospective” customer lists are compiled from information that is readily ascertainable to the public, such lists are not considered trade secrets).

To qualify as a trade secret, information must not only derive independent economic value from not being generally known or readily ascertainable, but it must also be “the subject of efforts that are reasonable under the circumstances to maintain its secrecy.” *See* §688.002(4)(b), Florida Statutes. Moreover, the employer bears the burden of proving that the information it seeks to protect is in fact secret and that it has taken reasonable steps to protect the secrecy. *See* *American Red Cross v. Palm Beach Blood Bank.* Significantly, several courts have found that customer lists and information about customer activity such as purchasing history and pricing information on items ordered constituted traded secrets. For example, in *Sethscot Collection, Inc. v. Drbul*, the Court held that a list containing customers that had ordered customized clothing in the last eight years and included a purchasing history of each customer list was a trade secret. Similarly, in *Thomas v. Alloy Fasteners, Inc*., the Court concluded that order edits lists that included the mark-up on the items ordered and the profit margin was a trade secret.

 An employer may obtain an injunction to prevent the actual or threatened misappropriation of its trade secrets. *See* §688.003(1). The injunction will normally terminate when the trade secret ceases to exist. However, a court may continue the injunction for as long as is necessary to eliminate the unfair advantage derived from the misappropriation. The employer may also recover monetary damages such as lost profits, damages for unjust enrichment, and “exemplary” damages if a court determines that the misappropriation was willful and malicious. *See* §688.004(2), Florida Statutes.

 **F. Restrictive Covenants**

 *1. Background*

 The most effective and efficient way to protect against unfair competition and the improper use of confidential information is through the use of restrictive covenants. Restrictive covenants are agreements that limit certain activities by the employee either during or after the employment relationship. Such agreements include non-competition covenants, non-solicitation covenants, anti-piracy agreements, and confidentiality and non-disclosure agreements.

 The use and enforcement of restrictive covenants has been the subject of great debate. Historically, restrictive covenants such as non-compete provisions were viewed as being contrary to the free enterprise system, which revolves around competition among businesses. Even today, the basic policy in Florida is still in favor of competition. Thus, mere competition for business by a competitor typically is not actionable, and a non-compete agreement cannot be used as a tool simply to eliminate competition. Over time, however, the Legislature and Florida’s courts have realized that employers should be able to curtail unfair competition. These two competing interests -- free competition vs. unfair competition -- continue to create tension when employers seek to enforce restrictive covenants.

 In 1953, the Florida Legislature enacted its first non-compete statute to impose certain limited restraints on trade and to protect an employer’s proprietary interests. In 1996, the statute was repealed, except with respect to covenants entered into before July 1, 1996, and replaced by §542.335, Florida Statutes. In addition to being applicable to current and former employees of a company, restrictive covenants can also apply to partners, shareholders, agents, independent contractors, and sellers of all or part of a business. *See* §§542.33(2) and (3), Florida Statutes. It is significant to note that the new statute does not apply to restrictive covenants entered into, or having an effective date, prior to July 1, 1996.

 *2. Signature Required*

First, to be enforceable under 542.335, Florida Statutes, restrictive covenants such as non-compete provisions must be in writing and signed by the person to whom the restrictive covenant applies, which is typically an employee.

 *3. Consideration Required*

 Second, in addition to the requirement that the covenant be in writing and signed by the person against whom enforcement is sought (i.e., the employee), Florida law requires that the restrictive covenant be supported by adequate consideration. *See Wright & Seaton v. Prescott*. Essentially, this means that the employee or applicant must be provided with something of value in exchange for signing the agreement. The consideration is satisfied where the covenant was signed by the employee at the onset of the employment relationship, where the covenant was signed by the employee after the employer provided a salary increase, or where the covenant was signed by the employee in exchange for continued employment. *See Criss v. Davis, Presser & LaFaye; Coastal Unilube Inc. v. Smith.*

 *4. Restrictive Covenant Types*

There may be multiple types of restrictive covenants contained in an agreement between employer and employee. Some employment agreements may contain some, but not all, types of restrictive covenants. Such restrictive covenants include non-competition agreements, non-solicitation agreements, confidentiality agreements, and anti-piracy agreements. A non-competition agreement is broader than a confidentiality agreement or non-solicitation agreement and specifies prohibitions in subsequent employment, including possible prevention of the employee from working for a competitor in the same industry. A non-solicitation agreement may also prevent the individual from soliciting customers or clients once the individual ceases performing services or is no longer employed. An anti-piracy agreement prohibits a former employee from attempting to lure away the employer’s current employees.

 Courts appear to be more reluctant to enforce non-compete agreements than they are to enforce non-solicitation, anti-piracy, or confidentiality agreements. In *Edwards v. Harris*, the Court explained that restrictive covenants “cannot be used as a tool simply to eliminate competition.” An employer “cannot by contract restrain ordinary competition. In order for an employer to be entitled to protection, there must be special facts present over and above ordinary competition.” *See Passalacqua v. Naviant, Inc.* Rather than completely barring an employee from working for a competitor, many judges exercise their discretion to fashion what they view as a less drastic solution to address the former employer’s concerns. However, courts will enforce non-compete provisions where there are good reasons for doing so, and where less drastic measures will not sufficiently address the situation. The vast majority of cases upholding non-competes do so on the basis of exposure to trade secrets or confidential business information.

 Courts are more receptive to enforcing non-solicitation agreements, which prohibit the former employee from contacting any of the former employer’s customers. *See Advantage Digital Systems, Inc. v. Digital Imaging Services, Inc.*; *Austin v. Mid State Fire Equipment of Cent. Florida, Inc.* However, many courts have concluded that where a customer initiates contact with a former employee and seeks out his or her products or services at the new employer, does not violate a non-solicitation agreement. Simply put, the former employee did not solicit the customer. Rather, it the customer who solicited goods or services from the former employee. For that reason, employers that rely upon non-solicitation agreements with employees should include a restrictive covenant in the agreement that would prohibit the employee from performing services for or providing goods to the employer’s customers after severance of the employment relationship.

 *5. Breach of the Covenants*

 To obtain an injunction against a former employee to enforce the terms of a restrictive covenant, the employer must first prove that the former employee actually violated the terms of the restrictive covenant. This may seem obvious, but employers often lose sight of the fact that they must be able to present proof, in the form of admissible evidence in court, that the former employee actually violated the terms of the restrictive covenant. That may require that the employer’s customers be contacted and involved in any litigation to enforce the restrictive covenant.

 *6. Legitimate Business Interests*

 Additionally, the party seeking to enforce a restrictive covenant (i.e., the employer) must show that it has legitimate business interests that justify the existence and enforcement of the restrictive covenant. For example, as previously noted, merely wanting to eliminate competition is not a legitimate business interest that will support enforcement. On the other hand, a non-disclosure agreement is entirely appropriate for a Coca-Cola employee who has access to the secret formula, and a non-solicitation agreement is appropriate for a salesperson who works major accounts. Section 542.335(1)(b) provides a non-exhaustive list of “legitimate business interests,” which includes: (1) trade secrets as defined in §688.002(4), Florida Statutes; (2) valuable confidential business or professional information that otherwise does not qualify as trade secrets; (3) substantial relationships with specific prospective or existing customers, patients, or clients; (4) customer, patient, or client goodwill; and (5) extraordinary or specialized training. *See Fulford v. Drawdy Brothers Construction* (stating that there is a legitimate business interest in customer lists); *Colucci v. Kar Kare Automotive* (finding that protectable information includes that which is unique in the industry and confidential); and *Kupsczak v. Blasters* (stating that the unique methodology of a contractor’s highway paint stripe removal was a trade secret or, at a minimum, confidential business information).

  *7. Temporal and Geographic Scope*

In some states, restrictive covenants that are too broad in terms of their geographic scope or duration are void and unenforceable. Fortunately, in Florida, such is not the case. Instead, a restrictive covenant that is subject to Florida law may be “blue penciled” by a court. That is, if the court concludes that the restrictive covenant covers a geographic area that is unreasonably large and/or is too long in duration, the court can simply reduce the duration of the restrictive covenant and/or reduce the size of its geographic scope, rather than altogether refuse to enforce it.

In Florida, time limits of two years or less have typically been deemed reasonable, whereas time restrictions of more than two years have been found to be unreasonable. *See Capelouto v. Orkin Exterminating Equipment;* and *Southernmost Foot & Ankle Specialists, P.A. v. Torregrosa.* Section 542.335 sets forth specific presumptions of enforceability with regard to time limitations. Specifically, where a restrictive covenant is not predicated upon the protection of trade secrets, but is sought to be enforced against a former employee, agent, or independent contractor, and the covenant is not associated with the sale of assets, shares, partnership interest, equity interest, or a limited liability company membership, the court shall presume reasonable in time any restraint of six (6) months or less in duration and shall presume unreasonable any time restraint more than two (2) years in duration. *See* §542.335(1)(d)1. Where the restrictive covenant is not predicated upon the protection of trade secrets, but is sought to be enforced against a former distributor, dealer, franchisee, or licensee of a trademark, and the covenant is not associated with the sale of assets, shares, partnership interest, equity interest, or a limited liability company membership, the court shall presume reasonable in time any restraint of one (1) year or less in duration and shall presume unreasonable any time restraint more than three (3) years in duration. *See* §542.335(1)(d)2. Finally, where the restrictive covenant is not predicated upon the protection of trade secrets, but is sought to be enforced against the seller of assets of a business, shares of a corporation, a partnership interest, an equity interest in a business, or a limited liability company membership, the court shall presume reasonable in time any restraint of three (3) years or less in duration and shall presume unreasonable any time restraint more than seven (7) years in duration. *See* §542.335(1)(d)3, Florida Statutes.

With regard to geographic scope, courts look at the particular facts of each case to determine whether the territorial restraint is reasonably necessary to protect the employer’s interests. Factors such as the area in which the company does business and/or the area in which the employee worked are relevant in determining whether the geographical scope is enforceable. For example, in *Supinski v. Omni Healthcare, P.A.,* the court upheld a restriction prohibiting a physician from practicing within a ten (10) mile radius of any of three medical offices within a county. Meanwhile, the court in *Open Magnetic Imaging v. Nieves-Garcia*, determined that a restriction prohibiting a physician’s representative from working in all three counties where the employer had medical offices was overly broad, when the representative had worked in only one county. Similarly, in *Cerniglia v. C & D Farms,* the Florida Supreme Court held that a nationwide restriction on competition was too broad.

**G. Reasonable Employer Actions to Retain Information Secrecy**

 *1. Security Program*

Companies suffer the most serious leaks of confidential information from their employees and contractors. To prevent such loss of confidential/trade secret information companies must devise a comprehensive security program for its confidential information and ensure that the program is consistently followed. Such evidence that a security program exists, is consistently followed, and updated regularly will be used to demonstrate the employer has taken reasonable efforts to maintain the secrecy of trade secrets and other confidential proprietary information. This evidence will form the basis of necessary evidence for the offensive causes of actions listed above, requiring the employer show that it took reasonable efforts to maintain the secrecy of the information. Such a security program first requires an inventory be performed to determine all of the confidential and trade secret information the company has and who has access to it. This may require writing down information that currently is in only one or two employees’ heads and could be lost whenever the employees decided to leave the company. This security program also requires development of a company-wide confidentiality policy that does not violate the NLRA. It also requires development of a company-wide document retention and disposal policy, restricting access to confidential/trade secret computer drives only to those with a “need to know” such information and detailed confidentiality agreements. It may also require development and execution of non-compete and non-solicitation agreements with provision for injunctive relief upon violation, a Bring Your Own Device (BYOD) Agreement, and an exit interview process that reminds employees of their non-disclosure obligations upon separation of employment.

 *2. Non-Disclosure Policy/Restrictive Covenant Agreements*

Employers who take information secrecy seriously have employees with access to such information. The timing of entering into a binding non-disclosure agreement is extremely important. Employees, contractors, or vendors requiring access to a trade secret or confidential proprietary information, should sign such binding agreements when the relationship warranting disclosure of secret information first begins, not at the end of such a relationship. Most individuals who realize that a relationship is about to end will refuse to sign such agreements and for good reason. Virtually, the only way to secure an employee’s cooperative execution of such an agreement towards that end of the employment relationship is to buy it. This can be very expensive for the company and is avoidable. In addition, employers failing to get an enforceable non-disclosure or confidentiality agreement will find it particularly difficult to demonstrate that reasonable measures were taken to prevent disclosure of the confidential [trade secret] information. Employers must ensure that the definition of confidential information in such agreements will cover all trade secrets and proprietary information, accessed by the employee. In other words, a standard agreement template will not necessarily fit all company employees

 *3. Document Retention Policy*

When a document retention policy is appropriate, the policy should be carefully crafted to delineate what categories of documents will be retained, how they will be retained and accessed, who will retain and access them, and for how long they will be retained. Part of the policy may provide that employees are not to use personal email for work purposes and no company documents may be forwarded to personal email addresses at any time. The policy should also specify that documents containing trade secret and confidential proprietary information may not be forwarded to personal emails, personal devices or those without a need for access. All documents containing trade secret and confidential proprietary information should be inscribed with a legend and/or logo indicating that they contain trade secret and confidential information. The decision will also need to be made if trade secret and/or confidential proprietary information will be encrypted and/or password protected. The policy should also provide for proper means of destruction of documents depending on the distinct categories of such documents. Proper monitoring of the confidential devices is necessary to give the policy teeth.

In addition, the policy should contain verbiage that provides that all documents used in the course of business and/or accessed during work operations, and even those considered “personal” are owned by the company. The first part of the policy will be used to demonstrate that reasonable methods were used to keep the employer’s trade secrets and confidential, proprietary information secret. The verbiage about all property belonging to the company is essential so that when conflict arises all information found by your IT expert on company data systems, can be used to prove the employer’s offensive legal causes of actions. When an employee is separated or resigns, have an exit system in place that reminds the employee of his obligation to the company. Monitor use and document management systems and consider exercising the company’s rights to remove the employee from contact with confidential information by separating the employee immediately, paying the employee’s notice period, or restricting access to important confidential data devices and monitoring the use of those devices.

 *4. Bring Your Own Device Agreement (“BYOD”)*

Today many employees, independent contractors and vendors come to work equipped with their own smart phones, tablets, and other personal devices. Employers permit such use to keep their overhead manageable and for employee convenience. Nevertheless, use of employees, independent contractors’, and vendors own devices increase the odds that breaches of company confidential proprietary and trade secret information will occur. To prevent such data breaches, employees, appropriate independent contractors, and vendors likely to have access and/or use such devices for work, should be required to sign a BYOD agreement. Such an agreement will require that upon notice or separation of employment or contract services or use of devices, the employee, contractor and/or vendor will bring their electronic devices to the IT department where examination for company documents will occur. Following IT’s examination and removal of any sensitive, confidential, or trade secret information, the devices will be returned to the owner.

**IV. CONCLUSION**

Although employers can take steps to monitor the behavior of their employees, those steps are not without limitations. Employers must be careful not to violate their employees’ legitimate rights to privacy. However, employees are not the only ones with privacy interests. Employers likewise have legitimate privacy interests that they can and should take steps to protect.

APPENDIX A

3813099v.1

1. The respective provisions provided in part:

… the Company’s…personnel…all personnel lists, rosters, personal information of co-workers…personnel information such as home phone numbers, cell phone numbers, addresses and emails addresses….

… you agree that you will not… publically criticize, ridicule, disparage or defame the Company…directors, officers, shareholders, or employees… [↑](#footnote-ref-1)
2. Investigative consumer reports are secured through personal interviews and have their own special rules that must be followed. 15 U.S.C. §1681d. [↑](#footnote-ref-2)
3. Disciplining employees for social media posts may also run afoul of the NLRA. [↑](#footnote-ref-3)
4. AR, CA, CO, CT, IL, LA, MD, MI, MT, NH, NJ, NM, NV, OK, OR, RI, TN, UT, VA, WA, WI, GU. [↑](#footnote-ref-4)