WORKPLACE CHALLENGES OF PRIVACY, SOCIAL MEDIA, AND TECHNOLOGY ISSUES

by

Cynthia N. Sass, Esquire

Sterling Education Services
Employment Law: Rights, Benefits, and Emerging Issues
January 18, 2017

Available Courtesy of:
SASS LAW FIRM
601 West Dr. Martin Luther King Jr. Boulevard
Tampa, Florida 33603
813. 251.5599
www.EmploymentLawTampa.com

WORKPLACE CHALLENGES OF PRIVACY, SOCIAL MEDIA, AND TECHNOLOGY ISSUES[1]

Cynthia N. Sass, Esquire[2]
SASS LAW FIRM
601 West Dr. Martin Luther King Jr. Boulevard
Tampa, Florida 33603
813.251.5599
www.EmploymentLawTampa.com

A. PRIVACY ISSUES

1. Employer's Right to Know vs. Employee's Privacy

a. **Court Cases Focus on the Reasonableness of Employee's Expectation of Privacy on a Case-by-Case Basis and the Employer's Electronic Communications Policy**. An employee's expectation of privacy in a workplace communication must be decided on a "case-by-case basis." *City of Ontario v. Quon*, 130 S.Ct. 2619 (2010). Notably, in its decision in *Quon*, the Supreme Court stated, "employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated." *Quon*, 130 S. Ct. at 2630. However, there has been some inconsistency with courts' rulings on such policies.

b. **Factors Considered**. In determining whether an employee had an expectation of privacy in communications sent or received on the employer's computer or electronic communications system, courts consider different factors:

- Does the corporation maintain a policy banning personal or other objectionable use?
- Does the company monitor the use of the employee's computer or email?
- Do third parties have a right of access to the computer or emails?
- Did the corporation notify the employee, or was the employee aware, of the use and monitoring policies?

---

[1] These materials are distributed by the Sass Law Firm for informational purposes only. These materials should not be considered legal advice and should not be used as such.

[2] Thank you to Yvette D. Everhart, Esquire of Sass Law Firm, for her assistance in preparing these materials.

See In re Asia Global Crossing, LTD., et al., 322 B.R. 247 (S.D. N.Y. 2005); *Kaufman, et al. v. SunGard Invest. Sys.*, 2006 U.S. Dist. LEXIS 28149 (D.N.J. May 9, 2006) (same).

c. **Cases Where No Expectation of Privacy Held Because of Employer Policy**.

- *Bingham v. Baycare Health System*, 2016 WL 3917513 (M.D. Fla. July 2016) (collecting cases that found no expectation of privacy based on an employer's policy).

- *Walsh v. Logothetis*, 2014 WL 229588 (E.D. Va. Jan. 2014) (even where the employer allows use of its computers for personal use, public employee had no reasonable expectation of privacy in government computer because the government's policy specifically stated that there was no expectation of privacy and retained the right to monitor use).

- *State v. Young*, 974 So. 2d 601 (Fla. 1st DCA 2008) ("where an employer has a clear policy allowing others to monitor a workplace computer, an employee who uses the computer has no reasonable expectation of privacy in it. In the absence of such a policy, the legitimacy of an expectation of privacy depends on the other circumstances of the workplace").

- *Leor Exploration & Production LLC v. Aguiar*, 2009 WL 3097207 at *4 (S.D. Fla. 2009) (whether the generic warning in an employer's handbook stating that all communications on an employee's computer can be monitored renders any expectation of privacy unreasonable must be decided on a case-by-case basis).

- *U.S. v. Hassoun*, 2007 WL 141151 (S.D. Fla. 2007) (employee had no reasonable expectation of privacy in any material on work computer where, although company policy did not forbid personal use of computer, it made clear that all uses, work or personal, would be subject to monitoring).

- *Muick v. Glenayre Elecs.*, 280 F.3d 741, 743 (7th Cir. 2002) (no reasonable expectation of privacy in workplace computer files where employer had announced that it could inspect the computer).

- *United States v. Simons*, 206 F.3d 392, 398 & n.8 (4th Cir. 2000) (no reasonable expectation of privacy in office computer and downloaded Internet files where employer had a policy of auditing employee's use of the Internet, and the employee did not assert that he was unaware of or had not consented to the policy).

- *Sporer v. UAL Corp.*, 2009 WL 2761329 (N.D. Cal. 2009) (employee had no expectation of privacy in computer usage where employer (1) had a policy of monitoring its employees' computer use; (2) warned employees that they had no expectation of privacy in email transmitted on the company system; and (3) provided its employees with a daily opportunity to consent to such monitoring by having to click through a warning to access the company system).

- *Thygeson v. U.S. Bancorp*, 2004 U.S. Dist. LEXIS 18863 (D. Or. Sept. 15, 2004) (no reasonable expectation of privacy in computer files and email where employee handbook explicitly warned of employer's right to monitor files and email).

- *Garrity v. John Hancock Mutual Life Ins. Co.*, 2002 U.S. Dist. LEXIS 8343 (D. Mass. May 7, 2002) (no reasonable expectation of privacy where, despite the fact that the employee created a password to limit access, the company periodically reminded employees that the company email policy prohibited certain uses, the email system belonged to the company, although the company did not intentionally inspect email usage, it might do so where there were business or legal reasons to do so, and the plaintiff assumed her emails might be forwarded to others).

d. **No Expectation of Privacy, Even Though Company Expressly Stated They WOULD NOT Monitor Employees' Email**.

- *Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996) (employee had no reasonable expectation of privacy despite assurances that email sent over the company email system would not be intercepted by management; when employee communicated a comment over email system utilized by entire company, a reasonable expectation of privacy was lost, and even if employee had a reasonable expectation of privacy, a reasonable person would not have considered employer's interception of communications to be a substantial and highly offensive invasion of privacy).

e. **Expectation of Privacy Where Employees NOT Informed About Monitoring**.

- *United States v. Slanina*, 283 F.3d 670, 676-77 (5th Cir.), vacated on other grounds, 537 U.S. 802, 154 L. Ed. 2d 3, 123 S. Ct. 69 (2002) (employee had reasonable expectation of privacy in his computer and files where the computer was maintained in a closed, locked office, the employee had installed passwords to limit access, and the employer "did not disseminate any policy that prevented the storage of personal information on city

computers and also did not inform its employees that computer usage and Internet access would be monitored").

- *Leventhal v. Knapek*, 266 F.3d 64 (2d Cir. 2001) (employee had reasonable expectation of privacy in contents of workplace computer where the employee had a private office and exclusive use of his desk, filing cabinets and computers, the employer did not have a general practice of routinely searching office computers, and had not "placed [the plaintiff] on notice that he should have no expectation of privacy in the contents of his office computer").

f. **Expectation of Privacy Even Where Employer Expressly States No Expectation Exists**.

- *Haynes v. Office of the Attorney General*, 298 F. Supp. 2d 1154, 1161-62 (D. Kan. 2003) (employee had reasonable expectation of privacy in private computer files, despite computer screen warning that there shall be no expectation of privacy in using employer's computer system, where employees were allowed to use computers for private communications, were advised that unauthorized access to user's email was prohibited, employees were given passwords to prevent access by others and no evidence was offered to show that the employer ever monitored private files or employee emails).

g. **Expectation of Privacy Despite Company's Electronic Communications Policy**.

- *Stengart v. Loving Care Agency, Inc.*, 973 A.2d 390 (N.J. 2009) (the New Jersey Supreme Court upheld the lower court's ruling that an employee's communications with her attorney that were on her former employer's company-issued laptop were protected by privilege, despite the employee's breach of the company electronic communications policy holding that the employee took reasonable steps to keep her emails to her attorney confidential by using her personal, web-based email account that was protected by a password she never shared with her employer).

- *U.S. v. Long*, 64 M.J. 57 (C.A.A.F. 2006) (despite the fact that user had to acknowledge a banner which stated that the computer system may be monitored and that evidence of unauthorized use collected during monitoring could be used for administrative, criminal, or other adverse action each time she logged on to use the computer, court held that plaintiff had a reasonable expectation of privacy in emails sent from her office computer and stored on the government server due in part to the fact she had a password known only to her).

h. **Electronic Communications Policies Can Be Used *Against* the Employer as Well**.

- *Helmert v. Butterball, LLC*, 2010 U.S. Dist. LEXIS 60777 (E.D. Ark. May 27, 2010) (court ordered Butterball to "search hard drives, laptops, and the personal email accounts" of two members of its upper management when Butterball failed to "explain why these accounts are not reasonably accessible or unlikely to lead to the disclosure of relevant information.")

2. <u>Off-the-Job Behavior, e.g., Blogging, Political Action, Intra-Office Dating</u>

a. **Liability for Discrimination in Electronic Communications**. "Harassment outside of the workplace may also be illegal if there is a link with the workplace, for example, if a supervisor harasses an employee while driving the employee to a meeting." *EEOC Enforcement Guidance: Vicarious Employer Liability for Unlawful Harassment by Supervisor* (June 18, 1999) http://www.eeoc.gov/Policy/docs/harassment.html.

1) <u>Cases on Employer Liability for Off-Duty Electronic Communications</u>.

i. **Facebook®**.

- *Fisher v. Mermaid Manor Home for Adults, LLC*, -- F. Supp. 3d – (2016), 2016 WL 3636021 (E.D. N.Y. June 2016) (finding that a post on Facebook® comparing an African-American employee to a character from the movie "Planet of the Apes" could create a hostile working environment and denying summary judgment where the employer was aware of the harassment but did nothing about it).

- *Meng v. Aramark Corporation*, 2015 WL 1396253 (N.D. Ill. Mar. 2015) (finding that sexually explicit graffiti posted about another employee on the Internet and Facebook®, among other things, such that a jury could reasonably determine it created an abusive work environment.)

- *Summa v. Hofstra University*, 708 F.3d 115 (2d Cir. 2013) (in plaintiff's gender discrimination and harassment case against the university where the football players, non-employees, made harassing posts on Facebook® page regarding a university employee, among other behavior, grant of summary judgment for the employer was proper because the employer took prompt action by removing the offender, addressing all complaints and providing

sexual harassment training to stop and/or prevent the harassing conduct by non-employees).

- *Terry v. Borough*, 2013 U.S. Dist. LEXIS 174584 (E.D. Pa. Dec. 13, 2013) (denying motion to dismiss race discrimination claim where plaintiff alleged that the employer treated him different after learning about his interracial relationship from wedding ceremony photographs plaintiff posted on his Facebook® page).

- *Amira-Jabbar v. Travel Services, Inc.*, 726 F. Supp. 2d 77 (D. Puerto Rico 2010) (plaintiff sued for hostile work environment based on a racist Facebook® photo comment made by a co-worker. The court held that the comment was sufficiently work-related because the photo was taken of a work-related outing to give rise to employer liability irrespective of whether the comment was posted during work hours or off duty.)

ii. **Blogs**.

- *Stewart v. CUS Nashville, LLC*, 2013 U.S. Dist. LEXIS 16035 (M.D. Tenn. Feb. 6, 2013) (denying summary judgment to employer for plaintiffs' retaliation claims where supervisors and management made negative and defamatory statements on a blog after the employees engaged in protected activity).

- *Espinoza v. County of Orange*, 2012 Cal. App. Unpub. LEXIS 1022 (Cal. Ct. App. Feb. 9, 2012) (a co-worker at a juvenile detention center started a blog on which other employees harassed plaintiff based on his disability. The jury awarded $820,700 in damages based on the employer's failure to take action against the blog following plaintiff's complaint.)

iii. **Surfing the Web**.

- *Burchell v. Unemployment Compensation Bd. of Review*, 848 A.3d 1082 (Pa. Commw. Ct. 2004) (finding plaintiff ineligible for unemployment where the employer terminated the plaintiff for putting pornography on employer's computers irrespective of whether they were placed on the computer during off-duty time).

iv. **Company Bulletin Boards**.

- *Blakely v. Continental Airlines, Inc. et al.*, 751 A.2d 538 (N.J. 2000)

(Continental operated a website where employees could log on to find flight times, schedules, etcetera. There was also a message board where co-workers posted derogatory and harassing messages about plaintiff. The court stated, "employers do not have a duty to monitor private communications of their employees; employers do have a duty to take effective measures to stop co-employee harassment when the employer knows or has reason to know that such harassment is part of a pattern of harassment that is taking place in the workplace." The message board was found sufficiently related to the workplace in order to hold the employer liable).

2) Unemployment. Florida's unemployment law defines "misconduct" to disqualify applicants from receiving unemployment benefits to include off-duty conduct if it is in disregard of the reasonable standards of behavior which the employer expects of employees.

- *See Fla. Stat. §443.036(30)* (an applicant may be disqualified from benefits for misconduct "irrespective of whether the misconduct occurs at the workplace or during working hours…").

3) Off-Duty Conduct Statutes. Florida does not have any statutes prohibiting employers from considering certain off-duty conduct (i.e. the use of lawful products like alcohol and tobacco). However, many other states do. To the extent an employer also has employees working in states other than Florida, it is important to check whether those states have off-duty conduct statutes.

4) Political Action.

i. **Employer Policy Restricting Protected Speech Violates First Amendment**.

- *Liverman v. city of Petersburg*, 2016 WL 7240179 (4th Cir. Dec. 15, 2016) (finding that employer's policy restricting use of social media violated the First Amendment's free speech clause. Policy prohibited employees from posting negative comments on the operations of the bureau, specific conduct of supervisors or peers that impacts public's perception of the department and discouraged employees from posting information regarding off-duty activities.).

ii. **Social Media Postings Protected Speech**.

- *Liverman v. City of Petersburg*, 2016 WL 7240179 (4th Cir. Dec. 15, 2016) (finding that disciplining officer employees for their posts and comments on Facebook® regarding promotional requirements

and criticizing placing inexperienced officers in higher ranking positions violated First Amendment Rights to free speech).

- *Garza v. Bolin*, 2016 WL 1714925 (W.D. Tex. March 2016) (denying summary judgment to employer where employee posted on Facebook® opposition to her employer's candidacy and was subsequently terminated for her Facebook® post and other political action).

- *Williams v. Madison County, Idaho*, 2014 WL 64773284 (D. Idaho 2014) (finding that Sheriff's termination of husband based on his wife's political speech on Facebook® supported an inference of retaliation for protected speech).

- *Bland v. Roberts*, 730 F.3d 368 (4th Cir. 2013) (terminating sheriff deputies for liking on Facebook® the sheriff's political opponent's campaign page violates the First Amendment).

- *Greer v. City of Warren*, No. 1:10-cv-01065, 2012 U.S. Dist. LEXIS 39735 (W.D. Ark. Mar. 23, 2013) (police officer's display of a confederate flag on MySpace™ page was protected speech).

iii. **Social Media Postings Not Protected Speech**.

- *Snipes v. Volusia County*, 2017 WL 3588273, --- F.3d --- (11th Cir. August 21, 2017) (Plaintiff's posting of racially insensitive comments on Facebook and in a group text was not protected speech under the First Amendment).

- *Gresham v. City of Atlanta*, 2013 U.S. App. LEXIS 20961 (11th Cir. Oct. 27, 2013) (law enforcement officer posting comment on Facebook® criticizing another co-worker was not protected speech because the government had a legitimate interest in maintaining discipline and good working relationships).

- *Graziosi v. City of Greensville*, 2013 U.S. Dist. LEXIS 172581 (N.D. Miss. Dec. 3, 2013) (finding that police officer's posts to Facebook® criticizing the department for not sending representatives to a fallen officers funeral were not protected speech).

- *Sheperd v. McGee*, 2013 U.S. Dist. LEXIS 159432 (D. Or. Nov. 7, 2013 (child caseworker's comments on Facebook® about purchase

choices of dependency clients were not protected speech).

- *Snyder v. Millersville University*, 2008 WL 5093140 (E.D. Pa. 2008) (there is no First Amendment protection for plaintiff/teacher's MySpace™ comments on private matters, not of public concern).

5) Other Restraints on Speech. Employer policies restricting political speech may constitute an unlawful policy in violation of the National Labor Relations Act. *See* Report of the General Counsel Concerning Employer Rules, pg. 11 (Mar. 18, 2015). Employers must be cautious about creating workplace rules that interfere with political speech if it could be directly related to employment-related concerns and employee concerted activity.

B. SOCIAL MEDIA ISSUES

1. Use of Social Networking Sites in the Employment Context: Risks, Best Practices, and Policies

a. **The Benefits of Using Social Media**.

1) Recruiting. Sixty percent of employers use social networking sites for recruiting purposes.[3]

2) Identifying Problems with Applicants; Investigative Tool. An employer may spot potential red flags such as pictures of the applicant engaged in drug use or other illegal acts.

3) Identifying Untruthfulness, Violations of Policies or Misuse of Sick Time. An employer may discover employee misconduct by reviewing social media. For example, social media might show that an employee was really at the beach or an amusement park on a day they called in sick. An employer may find in a comment or a post that the employee is violating one of the employer's policies while at work (e.g., a tweet saying "took a one-hour nap in the supply room again today").

[3] Careerbuilder.com, *Number of Employers Using Social Media to Screen Candidates Has Increased 500 Percent over the Last Decade* (April 28, 2016), available at http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?ed=12%2F31%2F2016&id=pr945&sd=4%2F28%2F2016.

4) Investigate Abuse of FMLA Leave.

- *Jones v. Gulf Coast Health Care of Delaware, LLC*, 2016 WL 659308 (M.D. Fla. Feb. 2016) (employer lawfully terminated employee based on Facebook® posts and text messages with co-workers showing the employee at amusement parks when the employee was supposed to be on medical leave for a shoulder injury).

- *Jaszczyszyn v. Advantage Health Physician Network*, 504 F.3d 440 (6th Cir. 2012) (employer lawfully terminated employee who allegedly was incapacitated and on FMLA for fraud where pictures of the employee drinking at a festival were posted on Facebook® and shared with management).

5) Evidence to Support Employment Decisions. Further, employers may use professional networking sites such as LinkedIn® to research an applicant's professional reputation.

6) Evidence of Violation of Agreements. Employers can use social media to research whether employees or former employees are living up to their employment and/or post-termination obligations, such as non-competition agreements, non-solicitation agreements, and confidentiality agreements, etcetera. Connecting with people on social media/networking sites, or updating or posting on social media/networking sites, may implicate restrictive covenants. There is no binding Florida authority regarding whether, and under what circumstances, a person's activity on social media/networking websites violates a restrictive covenant. However, the case law from other jurisdictions is instructive on this issue.

- *BTS, USA, Inc. v. Executive Perspectives, LLC*, 2014 WL 6804545 (Conn. Super. 2014) (defendant who left plaintiff-employer to work for competitor did not violate non-compete or non-solicitation agreement by updating his LinkedIn™ profile and encouraging his "connections" – which included clients of plaintiff – to check out competitor's new website; court noted that plaintiff "had no policies or procedures regarding employee use of social media," did not request or require ex-employees to delete their clients from LinkedIn® accounts, and did not discuss with defendant his LinkedIn® account in any fashion).

- *KNF&T Staffing, Inc. v. Muller*, Case No. 13-3676-BLS1 (Mass. Sup. Ct. Oct. 24, 2013) (updating LinkedIn® to change employment information did not constitute solicitation to violate non-competition and/or non-solicitation agreement).

- *Invidia, LLC v. Difonzo*, 2012 WL 5576406 (Mass. Super. 2012) (plaintiff hair salon sued its former hair stylist for breach of a non-solicitation agreement, citing that defendant had become Facebook® "friends" with eight of the plaintiff's clients since leaving and her Facebook® page announced her new employment with competitor; Court held defendant's conduct did not violate the non-solicitation agreement).

- *Coface Collections North America Inc. v. Newton*, 430 Fed. Appx. 162 (3d Cir. 2011) (granting employer an injunction against former employee who posted on Facebook® when his non-compete ended and encouraged former employees of employer to apply for a position with the plaintiff's competitive company).

- *Enhanced Network Solutions Group v. Hypersonic Technologies Corporation*, 951 N.E.2d 265 (Ct. App. Ind. 2011) (ENS contracted with Hypersonic and agreed that they would refrain from soliciting employees of each other. ENS posted a job opening on LinkedIn®, in which a Hypersonic employee applied on his own volition. The court found that posting an open position on the LinkedIn® webportal was not a violation of the non-solicitation agreement).

- *But see, Pre-Paid Legal Services, Inc. v. Cahill*, 924 F.Supp.2d 1281 (E.D. Okla. 2013) (finding that general posts on a former employee's personal Facebook® page promoting his new employer did not constitute solicitation of employees of the former employer and did not violate the non-solicitation agreement); and

- *TEKSystems, Inc. v. Hammernick*, Case No. 10-CV-00819 (D. Minn. Oct. 18, 2010) (employer sued former employee for solicitation based on former employee's connection on LinkedIn®; however, the case was dismissed without decision as the parties reached a settlement).

7) Other Notable Uses of Social Media and Technologies in the Workplace.

i. **Keystroke Logging Monitoring**. Keystroke logging software can be used to record the actual key strokes on an employee's computer in order to secretly determine what communications employees are having. Additionally, certain keystroke logging programs also take periodic screen shots and save them to a server or remote hard drive so that employers can monitor which websites employees are using. Such devices are legally

dubious. Presently, courts are reluctant to find that use of keystroke logging software violates the ECPA.

- *United States v. Barrington*, 648 F.3d 1178 (11th Cir. Fla. 2011) (use of software did not violate ECPA because this particular keylogging software did not contemporaneously capture and transmit keystroke-logging data beyond the user's computer).

- *Luis v. Zang*, 2013 U.S. Dist. LEXIS 29288 (S.D. Ohio Mar. 5, 2013) (no violation of the ECPA).

- *Klumb v. Goan*, 884 F. Supp. 2d 644 (E.D. Tenn. 2012) (no violation of the ECPA).

- *Rene v. G.F. Fishers, Inc.*, 817 F. Supp. 2d 1090 (S.D. Ind. 2011) (no violation of the ECPA, but plaintiff sufficiently pled SCA claim where defendant allegedly used keystroke-logging software to access plaintiff's email and financial accounts).

ii. **Radio Frequency Identification ("RFID")**. Use of RFID technology is increasing in the workplace. RFID allows employers to place incredibly small "tags" on items or people. RFID tags are most commonly attached to ID badges and security cards to grant access to secure areas. However, employers can also monitor the tags wirelessly to track employee behavior.

EXAMPLE: An employer may track how long it takes an employee to perform a certain task, when the employee arrives to and departs from work, or where in the building (or the city) an employee is located. RFID tags can also be tied to databases containing information about the individual, such as name, age, address, phone number, eye color, fingerprints, blood type, full medical history, etcetera.

iii. **Biometric Technologies**. On the rise is use of biometric technologies, such as palm scanning, fingerprints, and voice prints. They are often used as security functions on laptops, smartphones, etcetera. Some employers have been increasing the use of these biometric technologies in the workplace to track time and attendance, as well as to provide security and restrict access to certain areas in the workplace. Employers' use of these types of technologies implicates privacy concerns and may also give rise to discrimination claims. Another concern with using biometrics is the potential claims against the employer for identity theft. Some states, such as Illinois and New York, have laws regulating the use and collection of biometric data.

- *E.E.O.C. v. CONSOL Energy, Inc.*, 2016 WL 538478 (N.D. W. Va. Sept. 2016) (finding that an employer discriminated against and failed to reasonably accommodate an employee who believed the use of a biometric hand scanner conflicted with his religious beliefs).

iv. **Vehicle Monitoring Programs – EDR / GPS Devices**. Event data recorders ("EDRs") are designed to capture a range of information just prior to or during a crash event. For employees who drive as part of their job duties, some employers use EDRs or GPS devices to monitor the employees' vehicle movements and collect information regarding the employees' whereabouts or a potential collision event.

A. ***GPS Reports***.

- *Lochin v. Verizon Florida LLC*, 2010 WL 4056034 (M.D. Fla. Oct. 15, 2010) (employer used GPS reports from employee's vehicle to determine that employee was home approximately 20 hours a week).

B. ***Privacy Concerns***. Use of GPS devices can raise employee privacy concerns, particularly where the vehicle in question is employee-owned.

- *El-Nahal v. Yassky*, 993 F. Supp. 2d 460, 466 (S.D.N.Y. 2014) (no expectation of privacy in GPS data gathered on taxi driver's personal vehicles where the state regulatory authorities required tracking to be installed in all cabs.

C. ***Time Theft***.

- *Laba v. Chicago Transit Authority*, 2016 WL 147656 (N.D. Ill. Jan. 2016) (employer sufficiently stated a claim for unjust enrichment against employees where GPS tracking device showed employees using work time to perform non-work-related duties).

D. ***Event Data Recorders***. Most new cars come with EDRs standardly installed to capture data elements, such as speed, braking, use of a seat belt, and other information. 49 C.F.R. §563.5 defines EDRs as a device or function in a vehicle that records the vehicle's dynamic time-series data during the time period just prior to or during a crash event, but does not include audio and video data.

E. ***Driver Privacy Act of 2015***. Seeking to address these privacy concerns, the Driver Privacy Act of 2015 was enacted as part of the Fixing America's Surface Transportation Act (H.R. 22), and signed by President Obama on December 4, 2015 ("DPA"). The DPA provides

that, generally, data recorded or transmitted by an EDR may not be accessed by a person other than the vehicle's owner or lessee absent consent of the vehicle owner or lessee.

F. ***State Law***. As of Dec. 12, 2016, 17 states have enacted statutes relating to EDRs and privacy. Presently, Florida does not regulate the privacy of EDR. The states that do regulate EDR provide, among other things, that data collected from a motor vehicle EDR may only be downloaded with the consent of the vehicle owner or policyholder absent certain exceptions. See http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx.

G. ***Importance for Employers***. The vehicle monitoring programs of most employers apply to employees operating company-owned vehicles. In those cases, the employer owns or leases the vehicle and is consenting intuitively to accessing the data captured by EDRs. However, where employees use vehicles that they own or lease, employer access to EDR data requires the employees' written, electronic, or recorded audio consent under the federal Act.

H. ***Additional Implication of Vehicle Monitoring Programs***. If an employer obtains information by means of EDRs or GPS devices, this new knowledge has the potential to support a wage and hour claim as evidence of the employer's knowledge that the employee was performing uncompensated work.

- *Frew v. Tolt Techs. Serv. Group, LLC*, No. 6:09-CV-49-ORL-19GJK, 2010 WL 557940, at *5 (M.D. Fla. Feb. 11, 2010) (fact that employer regularly checked GPS records of employee's vehicle, as well as employee's employer-issued cell phone records, created a genuine issue of material fact as to whether the employer had notice that the employee was performing uncompensated overtime work).

b. **The Risks of Social Media**.

1) Potential for Discrimination. A potential employer can discover a wealth of information about an applicant, which they would not normally have, from various social media profiles including:

- Race/Color
- Age
- Religious Beliefs
- Sexual Orientation

- Memberships/Affiliations
- Political Associations
- Marital Status
- Parental Status

An employer could use this information to discriminate against an applicant for an unlawful purpose, or, even if the employer does not use the information, an applicant who was denied a position could still allege that they *did* use it.

i. *Nieman v. Grange Mutual Casualty Co.*, 2012 U.S. Dist. LEXIS 59180 (C.D. Ill. Apr. 2012) (allowing a plaintiff to proceed with an age discrimination claim where the plaintiff alleged that the employer learned of his age based on his graduation date from his LinkedIn® page).[4]

ii. *C. Martin Gaskell v. University of Kentucky*, No. 5:09-cv-00244-KSF (E.D. Ky. 2009) (no decision, settled out of court in January 2011 for $125,000, where employer performed an Internet search on a qualified candidate, discovered the candidate's religious beliefs, and decided not to hire the candidate, despite his superior qualifications, because of his religious beliefs).

2) Cyberbullying and Harassment. Employees, including managers, may use social media outlets to harass fellow co-workers or engage in cyberbullying of their co-workers. Thirty-five percent of working adults have reported being bullied at work.[5]

- *See Espinoza v. County of Orange*, 2012 Cal. App. Unpub. LEXIS 1022, (Cal. Ct. App. Feb. 9, 2012) (jury holds employer liable and awarded plaintiff over $820,700 in damages for cyberbullying and harassment. Employees posted to a non-employer blog reprehensible and hurtful comments about plaintiff's disfigured hand, which the employer had knowledge of but failed to take remedial action to correct).

3) Online Gripes By Employees. Employees may share negative or disparaging information about their working environment or relationships with co-workers. However, use caution if using such complaints to form the basis for discipline as some conduct may be protected activity as

[4] Ultimately, the pro se plaintiff lost his claims on summary judgment. *See Nieman v. Grange Mutual Casualty Co.*, 2013 U.S. Dist. LEXIS 47685(C.D. Ill. Apr. 2, 2013).

[5] Workplace Bullying Institute, *2010 & 2007 U.S. Workplace Bullying Surveys*, available at http://www.workplacebullying.org/multi/pdf/survey_flyer.pdf.

discussed below in Section 4.

4) False Information. An employer cannot be guaranteed that the information it receives from Internet sources is accurate. Potential candidates' profiles could contain undeserved glowing recommendations or harsh criticisms from friends and foes alike. Further, the person they describe themselves as online may not be an accurate portrayal of their true character, giving employers a false sense of familiarity with the candidate's true nature.

5) Employee Disclosure of Information. Employees may use social media to disclose an employer's proprietary information or other information that employers may not want publicly available or which may give rise to liability for the employer.

c. **Florida Computer Abuse and Data Recovery Act, Florida Statute §668.801 ("CADRA")**. Enacted in October 2015, CADRA protects the owner, operator, or lessee of a protected computer used in the operation of business, or the owner of the information stored on the protected computer, "from harm or loss caused by unauthorized access to such computer."

1) "Authorized User." Includes directors, officers, employees, third-party agents, contractors, or consultants of the owner, operator, or lessee of the protected computer or of the owner of information stored on the protected computer. Fla. Stat. §668.802(1).

2) "Computer." Defined as "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device that performs logical, arithmetic, or storage functions and includes any data storage facility, data storage device, or communications facility directly related to, or operating in conjunction with, the device." Fla. Stat. §668.802(3).

3) "Protected Computer." Defined as "a computer that is used in connection with the operation of a business and stores information, programs, or code in connection with the operation of the business in which the stored information, programs, or code can be accessed only by employing a technological access barrier." Fla. Stat. §668.802(6).

4) "Business." Includes for-profit or not-for-profit businesses.

5) Prohibited Acts. Under Florida Statute §668.803, a person is liable in a civil action if he or she knowingly and with intent to cause harm or loss:

- "Obtains information from a protected computer without authorization and, as a result, causes harm or loss;

- Causes the transmission of a program, code, or command to a protected computer without authorization and, as a result of the transmission, causes harm or loss; or

- Traffics in any technological access barrier through which access to a protected computer may be obtained without authorization[.]"

6) Damages. Under Florida Statute §668.804, the following damages are available:

- **Actual damages**, including the plaintiff's lost profits and economic damages;

- The **defendant's profits** that are not already included in the computation of actual damages;

- **Injunctive or other equitable relief** from the court to prevent a future violation;

- Recovery of the **misappropriated information, program, or code**;

- **Reasonable attorneys' fees** to the prevailing party; *or*

- All **remedies otherwise available** for the same conduct under federal or state law.

7) Statute of Limitations. Within three years of the occurrence of the violation, the discovery of the violation, or when the violation should have been discovered with due diligence. Fla. Stat. §668.804(5).

d. **Florida Uniform Trade Secrets Act, Florida Statute §688.001, *et seq.* ("FUTSA")**. A violation of the FUTSA occurs where someone misappropriates trade secrets or threatens to misappropriate a trade secret.

1) Trade Secret. FUTSA defines a "trade secret" 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."

2) Remedies. Injunctive relief, actual damages, unjust enrichment damages, exemplary damages for willful and malicious misappropriation, and attorneys' fees. However, the rise in use of social media makes it more difficult to protect client contacts or customer lists, because those outlets provide public access to contacts which are connected on social media sites, such as LinkedIn® and Facebook®.

- *See Sasqua Group, Inc. v. Courtney*, 2010 U.S. Dist. LEXIS 93442 (E.D. N.Y. Aug. 2010) (finding that where contacts and customer information could be ascertained through an Internet search, such as LinkedIn®, Facebook®, etcetera, there was no protection to the customer list as a trade secret, especially if the employer does not take any steps to protect its customer lists).

e. **Employer Liability for Non-Disclosure**. The *Federal Trade Commission Guidelines* state that when there is a connection between a person endorsing a product and the seller of the product "that might materially affect the weight or credibility of the endorsement," the connection must be fully disclosed. 16 C.F.R. §255.5. Thus, an employer may be liable when its employees comment on the employer's services or products on blogs or social media/networking sites if the employment relationship is not disclosed.

f.

EXAMPLE: When an employee posts favorable or promotional messages to an online message board discussing the employer's product, knowledge of the poster's employment would likely affect the weight or credibility of the endorsement. Therefore, the poster should clearly and conspicuously disclose his or her employment relationship to the employer. Otherwise, the employer may face liability for the post. *See* 16 C.F.R. §255.5.

g. **Legal Considerations**.

1) Regulations. The laws regulating it (*see also* Section 4 below).

2) Potential Violation of the Fair Credit Reporting Act, 15 U.S.C. §1681, *et seq.* ("FCRA"). The FCRA requires that employers notify applicants if consumer reports will be used in an employment decision.

i. **Consumer Report**. This phrase means any written, oral, or other communication of **any** information by a consumer reporting agency bearing on a 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.**

ii. **Consumer Reporting Agency**. A consumer reporting agency means any person, who for fees, dues, or on a cooperative non-profit basis, regularly collects and evaluates consumer credit information for purposes of providing reports to third parties. 15 U.S.C. §1681a(f).

- *See Sweet v. LinkedIn Corporation*, 2015 WL 1744254 (N.D. Cal. Apr. 2015) (found that LinkedIn® was not a consumer reporting agency for purposes of the FCRA.).

iii. **Employment Purposes**. This term is defined as a report used for the purpose of evaluating a consumer for employment, promotion, reassignment or retention as an employee.

iv. **Obligations BEFORE Obtaining Consumer Report**. The statute provides that in general, "a person may not procure a consumer report, or cause a consumer report to be procured, for employment purposes with respect to any consumer," unless:

- Written disclosure and notice are given to applicants that a consumer report will be procured for employment purposes, which must be made before the consumer report is obtained; and

- The applicant has given written consent or authorization to obtain the consumer report.

v. **Obligations BEFORE Taking an Adverse Action**. Generally, before rejecting an applicant based on information in a consumer report, employers must provide:

- Notice of the adverse action and a copy of the consumer report used to make that decision; and

- A copy of *A Summary of Your Rights Under the Fair Credit Reporting Act*. This summary can be obtained from the consumer reporting agency that provided the report or from the Federal Trade Commission's ("FTC") website. This will allow the applicant to review the report and notify the employer if it is accurate. See 15 U.S.C. §§1681b(b)(3)(A)(i) & (ii).

vi. **Obligations AFTER Taking Adverse Action**. After taking an adverse action against an applicant based on a consumer report, the employer

must provide notice to the applicant of the adverse action orally, in writing or electronically, and provide the following:

- The name, address, and phone number of the agency providing the consumer report;

- Notice that the consumer reporting agency did not make the decision to take the adverse action and that the consumer reporting agency will not be able to provide specific reasons for the adverse action;

- Notice of the applicant's right to obtain a free copy of the consumer report from the consumer reporting agency pursuant to Section 612 of the FCRA and that the applicant has 60 days to request it from the consumer reporting agency; and

- Notice of the applicant's right to dispute with the consumer reporting agency the accuracy of the information in the consumer report.

See 15 U.S.C. §1681m.

vii. **Penalties for Noncompliance**. Civil penalties include a $1,000 fine, punitive damages and the award of attorney's fees and costs.

viii. **Applicability**. The FCRA is typically inapplicable because employers tend to do their own searches of social media sites. However, if an employer were to employ an outside firm, or "consumer reporting agency" such as Info Check USA, to research the candidate's social networking profiles, the FCRA may require that the candidate is first given notice.

ix. **Treat Same as a Consumer Report**. Due to a dearth of case law on the subject, employers should err on the side of caution by treating social media searches as they would a consumer report or background check under the FCRA. If employers are going to search a candidate's social media profiles, they should inform the candidate, ask for permission (unless not permitted by state law), and give the candidate the opportunity to dispute negative information.

- In June 2012, the FTC entered into a settlement with Spokeo™, an online data banker. The FTC alleged that Spokeo™ constituted a

consumer reporting agency and it violated the FCRA when it marketed information to recruiters and employers.[6]

- In 2009, the city of Bozeman, Montana made news by requiring applicants to "Please list any and all, current personal or business websites, web pages or memberships on any Internet-based chat rooms, social clubs or forums, to include, but not limited to: Facebook, Google, Yahoo, YouTube.com, MySpace, etc." The form also asked for the applicant's user names, log-in information and passwords. While no lawsuits were filed, after much public criticism of the policy, the city eliminated the requirement.

3) Violations of the Fair Labor Standards Act of 1938 ("FLSA"). If a company instructs or allows a non-exempt employee to perform work on a company-sponsored social media page, the hours may be compensable and may constitute overtime, even where they are performed during non-business hours and off the job.

   - *Frew v. Tolt Techs. Serv. Group, LLC*, No. 6:09-CV-49-ORL-19GJK, 2010 WL 557940, at *5 (M.D. Fla. Feb. 11, 2010) (fact that employer regularly checked GPS records of employee's vehicle, as well as employee's employer-issued cell phone records, created a genuine issue of material fact as to whether the employer had notice that the employee was performing uncompensated overtime work).

4) State Laws that Impact the Use of Social Media in Hiring. In August and November 2015, Florida proposed bills (S.B. 186 and H.B. 635) prohibiting employers from requesting social media password information or retaliating against individuals who refuse to give social media password information. Unfortunately, neither passed. Notably, other states have passed legislation to prevent employers from requesting social media password information from prospective employees and current employees. If you have offices or employees throughout the United States, make sure you check the state's current legislation regarding this issue. You can also refer to the National Conference of State Legislators, *Access to Social Media Usernames and Passwords* available at: http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx

[6] *See Spokeo to Pay $800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA*, Fed. Trade Commission (June 12, 2012) (available at http://www ftc.gov/opa/2012/06/spokeo.shtm).

g. **Liability for Employee On-the-Job Misuse of Social Media**.

- *Doe v. XYZ Corp*., 887 A.2d 1156 (N.J. Super. A.D., 2005) (a mother, on behalf of her daughter, brought negligence action against her husband's employer for failing to properly prevent husband from maintaining and viewing child pornography on his work computer. The husband was emailing lewd photos of the daughter to a child pornography site. The court held that when an employer has actual or implied knowledge (in this case, the employer had actual knowledge of the husband's activities) that an employee is using his workplace computer to access pornography, possibly child pornography, and no privacy interest of the employee stands in the way, the employer is under a duty to investigate and effectively stop the employee's unauthorized activities, lest they result in harm to innocent third parties.)

h. **Minimizing the Risks**.

1) The best way to minimize risks is to implement and enforce a well-written electronic communications policy and/or social media policy as discussed in Section 3 below.

2) Give appropriate weight to information obtained from social networking sites based on the likelihood of reliability. If certain opinions or recommendations seem extraordinarily positive or negative, they probably are unreliable.

3) Google™ Alerts is a service offered by the search engine company Google™ that allows a user to monitor any content that is posted in news, blogs, or the web regarding a specific list of search terms which the user provides. Google™ Alerts can be used to monitor potential employees, clients, references to the company, etcetera.

4) Perform a search of candidates' social media in-house. This will eliminate the need to comply with the FCRA to inform the candidate before performing the search.

5) Have someone other than the decision-maker pre-screen the information and provide the decision-maker with only job-related information. This process will take advantage of the benefits of social networking research without exposing the company to liability for discrimination based on protected characteristics obtained from the search.

6) Make sure the employer is able to provide a legitimate, non-discriminatory reason for denying an applicant employment or taking certain employment actions.

7) Address ownership of social media accounts, the contents of the social media site as well as contacts at the time of hire, including an explanation regarding who owns the social media. Several courts have recently addressed whether an employer can assert an interest in social network accounts maintained by employees:

   - *Mattocks v. Black Entertainment Television, LLC*, 43 F.Supp.3d 1311 (S.D. Fla. Aug. 2014) (finding that a former employee had no property interests in the likes on a Facebook® page she initially created and later maintained for the employer).

   - *Eagle v. Morgan*, 2011 U.S. Dist. LEXIS 147247 (E.D. Pa. Dec. 22, 2011); 2012 U.S. Dist. LEXIS 143614 (E.D. Pa. Oct. 4, 2012); 2013 U.S. Dist. LEXIS 34220 (E.D. Pa. Mar. 12, 2013) (finding that former employee owned content to LinkedIn® account, but suffered no damages).

   - *Christou v. Beatport, LLC*, 849 F. Supp. 2d 1055 (D. Co. Mar. 14, 2012); 2013 U.S. Dist. LEXIS 9034 (D. Co. Jan. 23, 2013) (involving MySpace™ page, employee maintained MySpace™ page for employer during employment, employer sued for theft of MySpace™ friends after employee left and opened competing business; in July 2013, jury found in favor of defendant).

   - *PhoneDog, LLC v. Kravitz*, Case No. C11-03474, 2011 U.S. Dist. LEXIS 129229 MEJ (N.D. Cal. Nov. 8, 2011), 2012 U.S. Dist. LEXIS 10561 (N.D. Cal. Jan. 30, 2012) (involving Twitter account and employer's allegation that it owned the account upon employee leaving its employ; case settled and left question unanswered as to who owned the Twitter content).

8) Include social media policies in handbooks and review latest decisions by the National Labor Relations Board on appropriate social media policies.

9) When using social media as an investigative tool to obtain evidence of improper behavior justifying adverse employment actions, be sure to enforce the rules evenly. Use of social media investigative tools to punish one employee, while not similarly punishing a similarly situated employee

who engages in the same behavior can be used as evidence of discrimination.

10) Follow record retention requirements for applicants and/or employee files as set forth below in Section 3 below.

11) Incorporate language in social media policies as it relates to non-competition and/or non-solicitation activities post-separation.

12) Maintain confidentiality agreements and social media policies that explicitly address employee use of social media and confidential information. For example: What information constitutes confidential and/or proprietary information and restrictions for sharing on social media?

13) Make sure that the consequences for violation of the social media policy do not violate the NLRA.

14) Provide examples of both good and bad practices when using social media in the workplace.

15) Refer employees to one specific company official to discuss social media issues or answer questions.

16) Train all employees on the social media policies.

i. **Ensure Compliance with Record Retention Requirements**.

1) Federal Requirements. These remain unchanged even with the new advent of social media and on-line recruiting. *See* 29 C.F.R. §1602.12 (governing Title VII of the Civil Rights Act of 1964, 42 U.S.C. §2000e, *et seq.*, the Americans with Disabilities Act of 1990, as amended by the ADAAA, 42 U.S.C. §12101, *et seq.*, and Genetic Information Nondiscrimination Act of 2008, 42 U.S.C. §2000ff, *et seq.*); 29 C.F.R. §1627.3 (governing the Age Discrimination in Employment Act of 1967, 29 U.S.C. §621, *et seq*.); *see also* the FLSA, 29 U.S.C. §201, *et. seq.* (providing that every covered employer must keep certain personnel records for all non-exempt employees.)

2) Online Recruitment and/or Use of Social Media. The use of online recruitment or social media does NOT alter the employer's responsibility to preserve electronic data just as it would hard copies of employment applications, resumes, interview records, etcetera.

3) State Law Requirements. An employer may also have record retention requirements under state law as well.

EXAMPLE: In Florida, public employers, such as the state, counties, and cities, have an obligation to retain personnel records pursuant to the state public record laws. Employers should check their respective states to ensure whether any state record retention laws for employment records exist.

2. Posting Off-the-Clock Regarding Workplace Issues

a. Off-Duty Conduct. *See* Section 2 below.

b. National Labor Relations Act. *See* Section 4 below.

3. Monitoring and Creating Policies Regarding Internet, Email, Texting, and Other Electronic Communications. Monitoring social media and other electronic sources in the workplace raises numerous issues:

a. **Constitutional Protections**. Main constitutional protections related to social media/networking are the First and Fourth Amendments.

1) First Amendment. Social media postings by *public employees* may be protected First Amendment speech if the speech was of a public concern, not a personal concern, and the employee expressed such views as a private citizen and not in his or her official capacity. *Garcetti v. Ceballos*, 547 U.S. 410 (2006). *See also* Section 2 above.

2) Avoid Implementing Social Media Policies That May Have a Chilling Effect On Public Employees' Rights to Free Speech.

- *See Thomas v. Ladue Sch. Dist.*, No. 4:11-cv-1453 (E.D. Mo. 2011) (putative class action by teacher that school district's proposed policy preventing student-teacher communications and/or employee-student communications was a restraint on speech);

- *See also Mo. State Teachers Ass'n v. State of Missouri*, No. 11AC-CC00553 (Mo. Cir. Co. Aug. 26, 2011) (court-ordered injunction preventing school district from imposing the policy prohibiting student/teacher and/or employee communications find that it would have a chilling effect on free speech).

3) Fourth Amendment. Provides protection from *governmental* authority engaging in unreasonable search and seizures. Standard is whether the employee and/or applicant has a "reasonable expectation of privacy" in the

thing or matter searched.

- *See City of Ontario v. Quon*, 130 S. Ct. 2619 (2010) (where public employee had a reasonable expectation of privacy in electronic communications on employer devices, but the employer's search did not constitute an unlawful search and seizure. However, the Court in *Quon* held that an employee's expectation of privacy in a workplace communication must be decided on a "case-by-case basis").

- *State v. Young*, 974 So. 2d 601 (Fla. 1st DCA 2008) (where an employer has a clear policy allowing others to monitor a workplace computer, an employee who uses the computer has no reasonable expectation of privacy in it under the Fourth Amendment; in the absence of such a policy, the legitimacy of an expectation of privacy depends on other circumstances in the workplace).

b. **Laws to Be Aware of When Monitoring.**

1) The Computer Fraud and Abuse Act, 18 U.S.C. §1030 ("CFAA"). The CFAA prohibits unauthorized access of a computer or exceeding authorized access of a computer, when done to obtain information or damage computer functionality. Thus, a CFAA violation occurs if a defendant either (i) damages a computer system or (ii) obtains information to which he or she is not entitled.

i. **Purpose**. "[T]he CFAA was designed to target hackers who access computers to steal information or to disrupt or destroy computer functionality, as well as criminals who possess the capacity to access and control high technology processes vital to our everyday lives." *Trademotion, LLC v. Marketcliq, Inc.*, 857 F. Supp. 2d 1285, 1289-1290 (M.D. Fla. 2012) (quotations omitted).

ii. **Criminal and Civil Remedies**. The CFAA is primarily a criminal statute and provides criminal penalties, including fines and imprisonment for up to 10 years. However, the CFAA also provides a private right of action to "[a]ny person who suffers damage or loss by reason of a violation of this section' who 'may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. §1030(g). In a civil action, the plaintiff must demonstrate actual damages or loss resulting from the violation of the CFAA.

iii. **Protects Employers and Employees**.

A. ***Protects Employers***. A common situation that implicates the CFAA is when a departing employee attempts to gain an advantage by stealing information from the employer prior to his or her departure.

B. ***Protects Employees***. The CFAA can also apply when an employer attempts to access an employee's devices and steal information of the employee.

- *See, e.g.*, *Brooks v. AM Resorts, LLC*, 954 F. Supp. 2d 331, 332-333 (E.D. Pa. 2013) (former employee sued former employer for allegedly gaining unauthorized access to his computer and email account in violation of the CFAA).

iv. **Narrow Construction of Authorization**. Most jurisdictions—including Florida federal courts—have adopted a narrow construction of the CFAA that interprets "without authorization" or "exceeding authorization" as applying only to the defendant's ***access*** to the information in question, rather than the defendant's ***use*** of that information. Under the narrow construction, as long as the defendant was authorized to access the information, there is no CFAA violation regardless of the defendant's subsequent use of that information.

- *Enhanced Recovery Co., LLC v. Frady*, 2015 WL 1470852 (M.D. Fla. Mar. 2015) (continuing to recognize narrow definition of "exceeds authorization" as "while an employee's initial access was permitted, the employee accessed information for which the employer had not provided permission. Further, "exceeds authorization access" does not reach an employee who has actually been granted access to confidential information, but who accesses that information for the improper purpose of removing or disclosing the employer's information").

- *Trademotion, LLC v. Marketcliq, Inc.*, 857 F. Supp. 2d at 1287, 1290-1291 (M.D. Fla. 2012) (a claim could not be brought under the CFAA because employee had been granted full administrative access, regardless of how that access was used. "It is the employer's decision to allow or to terminate an employee's authorization to access a computer that determines whether the employee is with or 'without authorization.'").

- *Clarity Services v. Barney*, 698 F. Supp. 2d 1309, 1316 (M.D. Fla. 2010) (employee deleted information from his company laptop before returning the laptop to employer, and he read an email from a customer on employer's company email account after resigning from the company. The court dismissed employer's CFAA claim because employee was authorized to access the information and did not exceed his authorization.).

2) The Stored Communications Act, 18 U.S.C. §2701, *et seq.* ("SCA"). Prohibits intentionally accessing stored electronic or wire communications without authorization or in excess of authorization.

i. **Purpose**. Congress enacted the SCA "to protect privacy interests in personal and proprietary information from the mounting threat of computer hackers 'deliberately gaining access to, and sometimes tampering with, electronic or wire communications' by means of electronic trespass." *Devine v. Kapasi*, 729 F. Supp. 2d 1024, 1026 (N.D. Ill. 2010).

ii. **Criminal and Civil Remedies**. The SCA provides both criminal and civil causes of action and remedies. The possible criminal penalties include a fine and imprisonment for up to 10 years. 18 U.S.C. §2701(b). The civil remedies include injunctive relief, actual damages suffered by the plaintiff, any profits made by the violator as a result of the violation, punitive damages for willful or intentional violations, reasonable attorneys' fees, and other litigation costs reasonably incurred. 18 U.S.C. §§2707(b) and (c). The SCA provides a minimum recovery of $1,000 per person. 18 U.S.C. §2707(c).

iii. **Examples of Accessing Employees' Electronic Communications**. Performing searches of employees' email (particularly private email accounts where the log-in information may be saved on a company computer) or social media profiles may violate the SCA.

- *Owen v. Cigna*, 2016 WL 2997931 (N.D. Ill. May 2016) (finding that employee stated a claim for a violation of the SCA where employee alleged that the employer accessed her email account without her permission after she left the employ).

- *Ehling v. Monmouth-Ocean Hospital Service Corp.*, 961 F. Supp. 2d 659, 662-663, 665, 669-670 (D. N.J. 2013) (plaintiff-employee maintained a non-public Facebook® account that allowed only her Facebook® "friends" to view her wall posts. A co-worker who was

plaintiff's Facebook® friend took a screenshot of plaintiff's controversial Facebook® wall posts and provided them to management without any prompting by defendant-employer. Employer suspended plaintiff because of the posts, and she sued employer for violations of the SCA. The court held that plaintiff's non-public Facebook® wall posts were covered by the SCA because she "chose privacy settings that limited access to her Facebook wall to only her Facebook friends." Nevertheless, the authorized user exception applied where employee's co-worker/Facebook® friend provided unsolicited information to employer from employee's Facebook® page.).

- *Rodriguez v. Widener University*, 2013 U.S. Dist. LEXIS 84910, Case No. 13-1336 (E.D. Pa. June 17, 2013) (denying employer's motion to dismiss claims under the SCA and the Electronic Communications Privacy Act where employer allegedly accessed employee's Facebook® images and there was a factual issue as to how employer accessed or obtained the Facebook® images).

- *Snyder v. Fantasy Interactive, Inc.*, 2012 U.S. Dist. LEXIS 23087, Case No. 11 Civ. 3593 (WHP) (S.D. N.Y. Feb. 9, 2012) (employee stated a claim for violation of the SCA where employer accessed plaintiff's private Skype™ instant messages outside of the office).

- *Maremont v. Susan Fredman Design Grp.*, 2011 WL 6101949, at *5-6, No. 10 C 7811 (N.D. Ill. Dec. 7, 2011) (plaintiff was defendants' media marketing director and she maintained Twitter and Facebook® accounts for her personal use as well as to promote defendants' business. While plaintiff was recuperating from an automobile accident, defendants allegedly accessed her Twitter and Facebook® accounts without her permission and posted to these accounts in her absence. The court denied defendants' motion for summary judgment on plaintiff's subsequent claim for violations of SCA.).

- *Shefts v. Petrakis*, 2011 U.S. Dist. LEXIS, at *16, No. 10-cv-1104 (C.D. Ill. Nov. 29, 2011) (a party cannot avoid SCA liability by hiring a third party to access and copy stored electronic communications even if the files are not opened or read).

- *Rene v. G.F. Fishers, Inc.*, 817 F. Supp. 2d 1090 (S.D. Ind. 2011) (plaintiff sufficiently pled SCA claim where defendant allegedly

used keystroke-logging software to access plaintiff's email and financial accounts).

- *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548 (S.D. N.Y. 2008) (employer's access of employee's personal emails was unauthorized, and thus violated the SCA).

- *Pietrylo v. Hillstone Restaurant Group*, 2008 WL 6085437 (D. N.J. 2008) (plaintiff, an employee of Houston's Steakhouse, created a MySpace™ page and stated that its purpose was to operate as a place to "vent about any BS we deal with [at] work without any outside eyes spying in on us. This group is entirely private, and can only be joined by invitation." Plaintiff went on to state, "[l]et the s**t talking begin." At some point, a Houston's manager asked one of the members of the group to provide her MySpace™ password so that he could access the group. The employee stated that she gave him the password because she feared she would get in trouble if she did not. The jury found that defendant violated the SCA when it accessed the group without authorization.).

iv. **Fraudulent Authorization/Access**. When searching a potential candidate's social media profiles, any "friending" of the person under false pretenses or using someone else's social media profile to gain access to their private information may violate the SCA.

- *See Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 883-884 (9th Cir. 2002) (although the case did not involve pre-employment research, in *Konop*, a group of Hawaiian Airlines pilots was using an online bulletin board to discuss work-related matters. One of the employer's management members falsely posed as a pilot to gain access to the group. The Ninth Circuit held that in gaining access to the group by false pretenses, the employer violated the Federal Wiretap Act, the SCA, and the Railway Labor Act.).

3) The Electronic Communications Privacy Act, 18 U.S.C. §2510, *et seq.*("ECPA"). Title I of the ECPA, a/k/a the Federal Wiretap Act, regulates the search and seizure of electronic communications while they are in transit. The ECPA prohibits the unlawful interception, disclosure, or use of electronic communications; and it most often arises in the labor context where employers monitor and intercept communications between employees.

i. **Criminal and Civil Remedies**. The ECPA provides for criminal penalties including a fine and imprisonment for up to five years. 18

U.S.C. §2511(4). The following remedies are available in a private civil cause of action: injunctive and declaratory relief, declaratory damages, punitive damages, reasonable attorney's fees and other litigation costs reasonably incurred. 18 U.S.C. §2520. The ECPA provides that the plaintiff will receive at a minimum $10,000, regardless of a showing of any actual damages. 18 U.S.C. §2520(c)(2)(B). In addition, if the communication involves certain radio or private satellite video communications, the violator may be subject to suit by the federal government. 18 U.S.C. §2511(5).

ii. **Consent**. Under the ECPA, consent to the interception by one party to the communication is a defense to a violation.

iii. **Interception**.

- *Shefts v. Petrakis*, 2012 U.S. Dist. LEXIS 130542 (C.D. Ill. Sept. 13, 2012) (in an action between owners of a telecommunications company, co-owners' conduct constituted interceptions in violation of the ECPA where they accessed plaintiff's Yahoo!®-based emails using a screen-capture software that took images of plaintiff's computer activities).

- *United States v. Szymuszkiewicz*, 622 F.3d 701 (7th Cir. 2010) (jury found violation of ECPA where employee went on his supervisor's computer while she was away and activated a "rule" on her email account so that any email that was sent to the supervisor was also forwarded to the employee).

iv. **No Interception**.

- *Ehling v. Monmouth-Ocean Hospital Service Corp.*, 872 F. Supp. 2d 369 (D. N.J. May 30, 2012) (dismissing claim under analogous state wiretap act against employer who accessed employee's private Facebook® page via another employee's account because the Facebook® posting accessed was in "post-transmission storage" and was not in the course of transmission when employer viewed it).

- *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 883-884 (9th Cir. 2002) (an airline pilot sued employer under the ECPA after a company executive, using log-in information for another employee, accessed the pilot's private website, which contained derogatory comments of upper management. The court held that viewing the website was not an interception as defined by the ECPA.).

4) Florida Statutes §934.03 – Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited. The Florida wiretap statute prohibits an individual from intercepting any "wire, oral or electronic communication." Any person who has their wire, oral, or electronic communication intercepted in violation of the statute has a private cause of action where they may seek preliminary or equitable or declaratory relief as may be appropriate, actual damages but not less than liquidated damages computed at a rate of $100 a day for each day of violation or $1,000, whichever is higher, punitive damages and a reasonable attorney's fee and other litigation costs reasonably incurred. Fla. Stat. §934.10. In contrast to the Federal Wiretap Act, Florida's wiretap statute provides that consent to the interception is a defense only if all parties consent. Additionally, violation of the statute may result in a first degree misdemeanor charge resulting in up to one year in jail.

   - *O'Brien v. O'Brien*, 899 So. 2d 1133 (Fla. 5th DCA 2005) (court found wife violated Florida Statute §934.03 when she installed software on husband's computer which intercepted emails, chat conversations and instant messages).

5) Florida Computer Crimes Act, Florida Statute §815.01, *et seq.* ("FCCA").

   i. **Purpose**. The FCCA was enacted as "a supplemental and additional statute" to the preexisting criminal statutes in order to "proscribe[] various forms of computer abuse." Fla. Stat. §815.02(5).

   ii. **Prohibits**. The FCCA prohibits offenses against intellectual property (§815.04), trade secrets (§815.045), and general computer hackers (§815.06). With respect to hackers, the FCCA makes it a felony to "willfully, knowingly, and without authorization" do any of the following:

      - Access or cause to be accessed any computer, computer system, computer network, or electronic device, §815.06(2)(a);

      - Disrupt, deny, or cause the denial of the ability to transmit data to or from an authorized user of a computer, computer system, computer network, or electronic device, §815.06(2)(b);

      - Destroy, take, or damage equipment or supplies used or intended to be used in a computer, computer system, computer network, or electronic device, §815.06(2)(c);

- Destroy, injure, or damage any computer, computer system, computer network, or electronic device, §815.06(2)(d);

- Introduce any computer contaminant into any computer, computer system, computer network, or electronic device, §815.06(2)(e); or

- Engage in audio or video surveillance of an individual by accessing any inherent feature or component of a computer, computer system, computer network, or electronic device, §815.06(2)(f).

iii. **Additional Civil Cause of Action**. In addition to a criminal cause of action, the FCCA provides the victim a civil cause of action "against a person convicted under this section for compensatory damages." Fla. Stat. §815.06(5).

6) Florida Security of Communications Act, Florida Statute §934.01, *et seq.* ("FSCA"). Makes it a misdemeanor to (1) either (a) intentionally access "without authorization a facility through which an electronic communication service is provided" or (b) intentionally exceed "an authorization to access such facility;" and (2) "thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system." Fla. Stat. §§934.21(1) and (2).

c. **Monitoring Issues with Government Employees**. As a general matter, the Fourth Amendment makes warrantless searches by the government per se unreasonable. However, there are certain exceptions to that rule, one of which is the special needs of the workplace. This issue arises in the employer-employee context most often where the government is the individual's employer. In order for a government employer to perform a warrantless search of an employee's electronic media the search must: (1) be motivated by a legitimate work-related purpose; and (2) not be excessively intrusive in light of the justification.

- *City of Ontario v. Quon*, 130 S. Ct. 2619, 2628 (2010) (the issue involved the city police department performing a search of officers' text messages sent and received on employer-issued pagers. The officers alleged that the search constituted a warrantless government search in violation of the Fourth Amendment. The court held that because the reason for the search (to see if officers, who were charged for service overages, were being unfairly charged money for pager use which was required by their job) was motivated by a legitimate, work-related purpose and the method in which the search was conducted was not overly intrusive in light of that reason, there was no Fourth Amendment violation.).

- *City of Coral Springs, Florida – AGO Opinion 2009-19* (when public entities themselves choose to use social media platforms such as Twitter or Facebook®, issues arise as to which parts of the social media become public records. In a decision regarding whether the City of Coral Springs, Florida could create its own Facebook® page, the Attorney General advised that the city did have the authority to establish a Facebook® page so long as the page was for a valid municipal purpose. Whether information on the Facebook® page would constitute a public record would depend on whether the information was made or received in connection with the transaction of official business by the city. Due to the fact that the purpose of the page must be a municipal one, it follows that the placement of material on the city's page would presumably be in furtherance of such purpose and in connection with the transaction of official business. Thus, it is likely that the information on the city's Facebook® page would be a public record. The issue as to whether the city's "friends'" Facebook® pages would be public records was not decided, but the Attorney General's Office did warn that if the city should choose to create a Facebook® page, it should be sure to warn all those who become its "friend" of the application and implications of the Public Records Law.).

Government employers should always be aware of the broad application of the "in connection with the transaction of official business" standard when deciding how to utilize social media.

d. **What are the Essential Elements for Creating an Effective Electronic Communications and/or Social Media Policy?**

1) Designated Contact. In order to avoid unforeseen issues, employees should be instructed to consult a designated member of management if they have any question with regard to permissible uses of technology.

2) Discipline Stated. Employees should be made aware of all levels of discipline, up to and including discharge, that may result from a violation of the employer's electronic communications policy.

3) No Privacy Expectations. It should be plainly stated that **employees have no expectation of privacy, in anything they do, on any employer-provided technology system or with any devices used for work purposes.**

4) Monitoring Advisory. Employees should also be advised that monitoring will occur to ensure compliance with the electronic communications policy.

5) Actual Monitoring. At least one court has held an electronic communications policy was ineffective where the employer did not *actually* monitor the communications.

   - *Curto v. Medical World Communications, Inc.*, No. 03CV6327 (E.D.N.Y. 2006) (although employer had an electronic communications policy allowing for monitoring, the court held that the employee still had reasonable expectation of privacy because employer rarely did in fact monitor the system, which lulled employees into a "false sense of security").

6) Employer's Right to Access. State that the employer owns the computer and other electronic communications systems and therefore may, at any time and for any reason, access the employee's computer (fax machine, scanner, voice mailbox, smart phone, etcetera).

7) Limitations. Place very clear limits on the permissible extent of personal use of employer-provided technology. This is particularly important to government employers whose employees' use of personal social media sites to conduct government business may convert the content of those sites to public records. (*See* AGO Opinion 2009-19 regarding the City of Coral Springs, Florida's desire to create its own Facebook® page.)

8) Prohibitions on Actions. Prohibit the forwarding of any emails or other documents from company servers to employees' personal email accounts or computers, unless employees are using BYODs. See Section C below. Be clear that any communication which occurs on company-provided electronic systems is company property.

9) Policy Controls – Not the Supervisor. Be very clear that the policy is the controlling authority with respect to the use of electronic communications. Employees should know that even if their supervisor tells them differently, they will be held accountable if they do not abide by the guidelines in the policy.

10) Specification of Devices. Be specific with respect to which electronic systems are covered under the policy (i.e., BlackBerrys, laptops, desktops, fax, scanning and copy machines, etcetera). Also advise employees that if they are unsure whether the policy applies to a specific electronic system, they should assume it does, and ask the designated member of management before assuming otherwise.

11) Adherence v. Liability. Inform employees of the purpose of adhering to electronic communications policy. If employees are helped to understand

the potential liability of an employer for their tweets, Facebook® comments, etcetera, they will better remember the policy before engaging in such behavior.

12) No Time Limit. Employers should also stress the lasting characteristic of electronic communications. Employees should understand that electronic communications can be stored for years, infinitely in fact, and retrieved in litigation long after they have forgotten their existence.

13) Rules and Laws. It is also advisable to make very clear that no electronic communication, under any circumstance may violate employer, state or federal rules or laws prohibiting discrimination, harassment, or any other workplace policy.

14) Uniform Enforcement. Make sure that the policy is enforced evenly across the board. Allowing certain employees, e.g., supervisors, to use employer-provided technology for certain purposes while others cannot, only serves to blur the line as to what is permissible and what is not, in addition to providing a possible basis for discrimination.

15) Former Employees. Ensure that all comments, recommendations, criticisms, etcetera of former employees come from the human resources department. Prohibit managers and supervisors from making comments about employees via LinkedIn®, Facebook®, or other social or professional networking sites.

16) Confidential Information. Prohibit employees from disclosing confidential information about the company or their co-workers, or from using the company name or logo in connection with any personal online communications.

17) Tracking Electronic Use. Be clear that the company reserves the right to track employees via the Internet, email and mobile phone use.

18) Access Limitations. Specify very clearly the purposes for which employees may access company computers. Circulating policy paperwork and employment contracts outlining when an employee has exceeded their authorization to use company computers to access or obtain certain information is a good method for protecting employers from computer-related employee fraud and abuse.

19) Signing Policy. Have employees acknowledge that they have read and reviewed the policy, and consent to the monitoring, and then have them sign the policy. This will help avoid liability where employees claim that they

were not aware of the policy's provisions. This should be done periodically, at the employee's hiring, and then perhaps annually or semi-annually, to ensure that employees are always aware of the policy's existence.

4) **Ensure Policy Does Not Violate the National Labor Relations Act ("NLRA")**. The National Labor Relations Board ("NLRB") has started filing charges against employers for violations of Section 7 of the NLRA regarding restrictions on concerted activity, maintaining a rule prohibiting all non-business use is facially overbroad. When developing electronic communications policies regarding email and Internet use, employers must be careful not to violate Section 7 by limiting employees' ability to openly discuss work-related concerns.

EXAMPLE: If an employer allows employees to use its email system to perform their job, the employer must also allow the employees to use the email system to communicate with co-workers about workplace grievances, union organizing, strikes, etcetera, unless the employer can justify a total ban on non-work use of email.

Purple Communications, Inc., 361 NLRB No. 126 (Dec. 2014).

See Section 4 below.

5) **Common Law Invasion of Privacy Considerations**. Florida recognizes three common law invasion of privacy claims: a) intrusion upon seclusion; b) appropriation of likeness; and c) public disclosure of private facts.

6) **Intrusion Upon Seclusion**. This term is defined as physically or electronically intruding into an individual's physical solitude or seclusion.

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

- *Armstrong v. H&C Communications, Inc.*, 575 So. 2d 243 (Fla. 5th DCA 1991).

The type of intrusion typically applies to places or things where one has a reasonable expectation of privacy, not public places.

- *Benn v. Florida East Coast Railway Company*, 1999 U.S. Dist. LEXIS 14314 (S.D. Fla. 1999).

7) **Public Disclosure of Private Facts**. This term is defined as "dissemination of truthful private information that a reasonable person would find objectionable" and which are not of a public concern.

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

- *Woodward v. Sunbeam Television Corp*, 616 So. 2d 501 (Fla. 3d DCA 1993).

8) **Appropriation of Likeness**. This term is defined as "the unauthorized use of a person's name or likeness to obtain some benefit."

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

   - *See also* Florida Statute §540.08 as to claims for exploitation, use or likeness of any commercial name or likeness.

   Presently, there is no case law in Florida regarding liability for invasion of privacy involving social media sites, such as Facebook®, MySpace™, LinkedIn®, etcetera.

9) **Other Jurisdiction Case Law: No Claim for Invasion of Privacy**

   - *Ehling v. Monmouth-Ocean Hosp. Serv.*, 2013 U.S. Dist. LEXIS 117689 (D.N.J. Aug. 20, 2013) (granting summary judgment for employer on employee's invasion of privacy claim where plaintiff's Facebook® friend voluntarily gave the information to management).

   - *Rodriguez v. Widener Univ*., 2013 U.S. Dist. LEXIS 84910 (E.D. Pa. June 17, 2013) (dismissing public disclosure of private facts and false light invasion of privacy claims where employee failed to plead that the employer publicized his Facebook® postings to the public in a way that would be highly objectionable to a reasonable person or that the information was not of a genuine concern of the public).

   - *Sumien v. CareFlite*, No. 02-12-00039-cv, 2012 Tex. App. LEXIS 5331 (Tex. App. July 5, 2012), *affirmed Roberts v. CareFlite*, 2012 Tex. App. LEXIS 8371 (Tex. App. Oct. 4, 2012) (no claim for invasion of privacy where employer viewed former employee's comment on another user's Facebook® wall).

4. The NLRB and Social Media Issues

a. **Violations of the NLRA**. Section 7 of the NLRA provides all non-supervisory employees the right "to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection." This protection is very

broad and **applies to all employees, whether they are members of a union or not, and to employers, whether they employ union members or not.**

1) Definition of "Employee". The NLRA defines an "employee" as **any employee,** including those whose work has ceased as a consequence of, or in connection with, any current labor dispute or because of any unfair labor practice, and who has not obtained any other regular and substantially equivalent employment. However, "employee" **does not include** any individual:

   - Employed as an agricultural laborer, or
   - In the domestic service of any family or person at his home, or
   - Employed by his parent or spouse, or
   - Having the status of an independent contractor, or
   - Employed as a supervisor, or
   - Employed by an employer subject to the Railway Labor Act, or
   - Employed by any other person who is not an employer as defined by the NLRA.

2) Definition of "Employer". The NLRA defines an "employer" as **any person** acting as an agent of an employer, directly or indirectly, but not including:

   - the United States or any wholly owned government corporation, or
   - any Federal Reserve Bank, or
   - any state or political subdivision thereof, or
   - any person subject to the Railway Labor Act as amended from time to time, or
   - any labor organization (other than when acting as an employer), or
   - anyone acting in the capacity of officer or agent of such labor organization.

3) Definition of Concerted Activity. Generally, the NLRA protects the rights of employees to engage in "protected concerted activity," which is when two or more employees take action for their mutual aid or protection regarding terms and conditions of employment. A single employee may also engage in protected concerted activity if he or she is acting on the authority of other employees, bringing group complaints to the employer's attention, trying to induce group action, or seeking to prepare for group action.[7] When an employee suffers an adverse employment action as a result

[7] The NLRB "*Rights We Protect – Employee Rights*," http://www.nlrb.gov/rights-we-protect/employee-rights.

of language that is posted on social media sites such as Facebook® or Twitter, the action may give rise to an unfair labor practice charge if the language posted is construed as concerted activity. Recently, there has been a trend with the NLRB to file charges in cases where an employee suffered an adverse employment action for language posted on the Internet.

4) Remedies for Violations of the NLRA. The most severe of the remedies afforded by the NLRA are provided to an employee who has been terminated for conduct which is protected by the NLRA. Such employees may be afforded reinstatement and back pay; however, there are no compensatory damages such as emotional distress provided by the NLRA. Employers who engage in violative conduct can be issued a cease and desist order and made to post NLRB notices in the workplace. If the violative conduct has resulted in an unfair election, the NLRB can order that the election be rerun. If an employer refuses to bargain with an elected representative, the NLRB can order that they bargain.

   i. **Examples of Unlawful Social Media Policies**.

   - *Chipotle Services, Inc*., Cases 04–CA–147314 and 04–CA–149551, 364 NLRB No. 72 (August 18, 2016) (finding that Chipotle violated the NLRA when it maintained an unlawful social media code of conduct; directed an employee to delete certain tweets he had posted on his Twitter account, among other things).

   - *Hoot Winc, LLC and Ontario Wings, LLC d/b/a Hooters of Ontario Mills*, NLRB Nos. 31-CA-104872, 31-CA-104874, 31-CA-104877, 31-CA-104892, 31-CA-107256, 31-CA-107259 (May 19, 2014) (Hooters had a social media policy prohibiting any post that "negatively affects, or would tend to negatively affect, the employee's ability to perform his or her job, the company's reputation, or the smooth operation, goodwill or profitability of the Company's business." The administrative law judge ("ALJ") determined that this policy failed to provide sufficient guidance on the rule's application and, thus, employees reasonably would conclude it precluded protected activities.).

   The NLRB rejected the following social media policies as impermissibly overbroad – emphasizing that these policies failed to adequately specify the types of information employees were prohibited from posting, failed to distinguish such information from protected speech, and failed to provide examples of social media content the employer would consider "appropriate," "professional," "respectful," or "unfavorable."

- *Lily Transp. Corp.*, Case No. CA-108618 (April 22, 2014) ("employees would be well advised to refrain from posting information or comments about [the company], the [company's] clients, [the company's] employees or employees' work that have not been approved by [the company] on the internet . . . . [The company] will use every means available under the law to hold persons accountable for disparaging, negative, false or misleading information or comments involving [the company] or [the company's] employees and associates on the internet.").

- *Durham School Servs., L.P.*, 360 NLRB No. 85 (April 25, 2014) (an employer who operated a fleet of school buses maintained a social media policy that urged employees to "limit contact with parents or school officials, and keep all contact appropriate" and required employees to keep "communication with coworkers . . . professional and respectful, even outside of work hours." The policy also threatened discipline for "[e]mployees who publicly share unfavorable written, audio or video information related to the company or any of its employees or customers.").

ii. **The NLRB Found the Following Social Media Policies to be Lawful**:

- "Do not make negative comments about our customers in any social media."

- "Use of social media on Company equipment during working time is permitted, if your use is for legitimate, preapproved Company business. Please discuss the nature of your anticipated business use and the content of your message with your supervisor and Human Resources. Obtain their approval prior to such use."

- *Southern Workers Organizing Committee v. Wendelta Inc. d/b/a Wendy's*, NLRB No. 10-CA-136824 (January 20, 2015) (you may not: "Create a blog or online group related to Wendy's (not including blogs or discussions involving wages, benefits, or other terms and conditions of employment, or protected concerted activity) without the advance approval of the Legal and Communications Departments. If a blog or online group is approved, it must contain a disclaimer approved by the Legal Department.").

1) Social Media Conduct.

- *Three D, LLC d/b/a Triple Play Sports Bar and Grille*, 361 NLRB No. 31 (August 22, 2014) ("liking" the Facebook® comments of a former employee—who posted disparaging comments about his supervisor—constituted dialog among employees about working conditions and was protected concerted activity under the NLRA.).

- *Hoot Winc, LLC and Ontario Wings, LLC d/b/a Hooters of Ontario Mills*, Nos. 31-CA-104872, 31-CA-104874, 31-CA-104877, 31-CA-104892, 31-CA-107256, 31-CA-107259 (May 19, 2014) (the ALJ found that Hooters could not terminate two of its employees for publicly criticizing their co-worker and manager on social media in violation of Hooters' policies.).

- *MikLin Enterprises, Inc., d/b/a Jimmy John's*, 361 NLRB No. 27 (Aug. 21, 2014) (Jimmy John's violated the NLRA when its supervisors were "encouraging employees to disparage an employee union supporter on Facebook." The NLRB found that certain statements made by the employer's agents on an anti-union Facebook® page—encouraging employees to harass an employee because of his union support—violated §8(a)(1).).

- *But see Richmond District Neighborhood Center*, Nos. 20-CA-091748 (Oct. 28, 2014). The NLRB held that a Facebook® conversation between two employees was so egregious that it lost protection under the NLRA, illustrating there are limits on what constitutes protected concerted activity in the context of social media. Two disgruntled employees took to Facebook® to complain about their supervisors and to discuss their plan to engage in insubordinate acts. The NLRB found that "the pervasive advocacy of insubordination in the Facebook posts, comprised of numerous detailed descriptions of specific insubordinate acts, constituted conduct objectively so egregious as to lose the Act's protection and to render [the employees] unfit for further service."

C. WIRELESS DEVICES AND EMPLOYEE'S AND EMPLOYER'S PRIVACY VIOLATIONS

1. **Privacy Considerations on Wireless Devices**.

   a. **Wireless Devices Provided by Employer**. Privacy considerations will be the same as those discussed in Section A of this outline.

1) Reasonable Expectation. What will control is whether the employee had a reasonable expectation of privacy on an employer's device, as well as whether the employer has a relevant policy in place.

CAUTION: Even when employees use employer devices, an employer reviewing an employee's personal emails or email account on the device may violate federal law.

- *See, e.g., Lazette v. Kulmatycki*, 2013 U.S. Dist. LEXIS 81174 (N.D. Ohio June 5, 2013) (finding that employer may violate the SCA when a supervisor accessed a former employee's personal email on a company-owned Blackberry and shared it with third parties.).

b. **Wireless Devices Provided by Employee**.

1) Bring Your Own Devices or "BYOD". There is an increasing trend of employees using personal devices (smartphones, tablets, etcetera) to perform company work.

2) Privacy and BYOD. BYOD implicates a balance between the employee's privacy and the employer's interest in protecting its company information, trade secrets, data, etcetera. Thus, employer policies and practices regarding BYOD must be carefully considered.

3) Examples of Employers Entitled to Search Employee Personal Devices.

- *Kamalu v. Walmart*, 2013 WL 4403903 (E.D. Ca. 2013) (employer had right to go into the personal cell phone records of an employee claiming discrimination, to support its defense that employee performed misconduct by misrepresenting her work hours; inquiries about phone records were limited to date, time, and duration of phone calls and text messages.).

- *Mintz v. Mark Bartelstein & Associates, Inc*., 885 F. Supp. 2d 987 (C.D. Ca. 2012) (employee who used his personal cell phone for work duties had a limited expectation of privacy concerning his phone records because the employer paid the phone bill; employee received an employee manual that included the policy on his use of the employer's equipment, but he did not read the manual or sign the acknowledgement form.).

4) Potential Risks of Permitting BYOD.

i. **Performance Management**. The intermingling of personal and

business use on employee devices may affect the productivity and performance of employees.

ii. **Preservation and Lack of Control over Company Information**. Employees using their personal devices create a challenge for employers to preserve any evidence on those devices in the event of litigation because they do not control the personal device, which is especially true once the employment relationship ends. Moreover, the use of BYODs can also make it difficult for employers to determine whether employees have misappropriated company information or trade secrets.

iii. **Wage and Hour Considerations**. Allowing non-exempt employees to use their personal devices for work could result in them "working" off the clock or after working hours, which may give rise to wage and hour claims.

iv. **Security Considerations**. BYOD use implicates significant security concerns, such as:

- Safeguarding company information in the event of lost or stolen devices and/or security breaches.

- Potential violations of HIPAA for protected health or medical data.

EXAMPLE: In December 2013, Adult & Pediatric Dermatology, P.C. paid a penalty of $150,000 and settled a HIPAA violation lawsuit resulting from the loss of an employee's unencrypted thumb drive, which contained information for over 2,200 patients. The thumb drive was stolen from the employee's car.

v. **Discrimination/Harassment**. Covered employers generally have an obligation to ensure that employees are not harassed or discriminated and/or retaliated against because of protected characteristics. Employee use of personal devices could perpetuate harassing, discriminatory, or retaliatory behavior towards other co-workers for which the employer may be liable (texting, photos, etcetera).

- *Leslie v. Cumulus Media, Inc.*, 814 F. Supp. 2d 1326, 1341 (S.D. Ala. 2011) (former employee asserted claims of sexual harassment/hostile work environment stemming from co-worker texting her a cartoon picture of a penis.).

5) Possible Employer Liability for Accessing Employee-Owned Device.

i. **Invasion of Privacy**. Again, the critical inquiry is whether the employee has a reasonable expectation of privacy in his or her personal device.

A. ***Fourth Amendment***. Provides protection from *governmental* authority engaging in unreasonable search and seizures. Standard is whether the employee and/or applicant has a "reasonable expectation of privacy" in the thing or matter searched. In determining whether a reasonable expectation of privacy exists, courts apply the two-prong test used in the Fourth Amendment constitutional context:

- First, an actual subjective expectation of privacy must exist.

- Second, the expectation of privacy must be one that is objectively reasonable.

B. ***State Constitutional Right to Privacy***. Florida's state constitution provides another source of privacy protection. Art. 1, Sect. 23 states: "Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein." Further, Florida's constitution construes a right against unreasonable searches and seizure with the Fourth Amendment of the United States Constitution. As a result, monitoring public sector employees in Florida requires balancing employee privacy rights with the employer's interests. Additionally, Florida imposes restrictions on surveillance beyond those established by federal law. *See* §934.03, Fla. Stat.

C. ***Common Law Invasion of Privacy Considerations***. Intrusion upon seclusion, appropriation of likeness; and public disclosure of private facts. See Section A above.

ii. **Violations of Federal and State Computer Trespass Statutes**. An employer's access of an employee's personal device may violate, or at least implicate, numerous federal and state computer trespass statutes, such as the CFAA, ECPA and/or the SCA.

- *But see*, *Rajaee v. Design Tech Homes, LTD*, 2014 WL 5878477 (S.D. Tex. Nov. 2014) (dismissing employee's claims under the ECPA and CFAA based on the employer accessing employee's personal smart phone and wiped data from the phone. Specifically, the Court found that personal data on the iPhone was not protected

under the ECPA and that the employee did not provide any evidence of loss under the CFAA that aggregates to at least $5,000.).

6) Tips for an Effective BYOD Policy.

i. **Establish Expectations and Requirements**.

- Establish expectations regarding employee use of personal devices at work, but avoid infringing upon employee freedoms and off-duty conduct.

- Address who controls the company-related information on the personal device and the employee's obligations with respect to an employer's need to access company information.

EXAMPLE: When litigation against an employer is anticipated or commences, employees using personal devices may have information or evidence on their personal devices relevant to the litigation that will require the employer to issue a litigation hold and/or preserve the information on the employee's personal device.

- Make it clear that the employer can prohibit, prevent, or revoke the employee's use of personal devices for work-related purposes at any time.

ii. **Prohibit Intermingling of Information**. Prohibit the intermingling of company and personal information on the device. For example, require separate email accounts on the device and/or separate folders or locations for company information and personal information.

iii. **Confidentiality Agreements**. Have employees who use their own personal devices to perform work sign confidentiality agreements to protect company information, trade secrets, etcetera, from disclosure to third parties.

iv. **Consent to Monitoring**. Reduce employees' expectation of privacy on their own personal devices and inform employees that their personal devices may be monitored or subject to search in specific circumstances (e.g., termination, to protect confidential or proprietary information, in the event of a litigation hold), and obtain written consent to monitor the employees' personal devices.

v. **Address Return of Information and Loss of Information**. Implement policies and procedures: (1) for the return of company information,

trade secrets, files, etcetera, on employee personal devices; and (2) for lost or stolen devices.

vi. **Post-Employment Agreements**. When an employment relationship ends, obtain an agreement regarding the employer's access to company information stored on the employee's personal devices. For example, an employer may want to incorporate these types of obligations in severance agreements.

7) Workplace Technology and Unwanted Information Disclosure.

i. **Data Breaches – A Significant Issue for Employers**. As recently reported by the *Wall Street Journal*,[8] a December 2015 survey[9] by the Association for Corporate Counsel revealed that one-third of in-house counsel have experienced a corporate data breach and more than half of in-house counsel report that their companies are increasing spending on cybersecurity.

ii. **Primary Causes of Data Breaches, i.e., Unwanted Information Disclosures**.

A. ***Employee Error***. The most common cause of data breaches are employee error (24% of reported data breaches). For example, an employee "accidently sending an email with sensitive information to someone outside the company."

B. ***Intentional and Malicious Access by Insiders***.

C. ***Phishing***. "Phishing" refers to when third parties send spam emails designed to trick employees into giving up their personal information.

D. ***Third-Party Access***.

E. ***Lost Device***.

F. ***Malware***.

iii. **Primary Employer Victims of Data Breaches**. According to the survey, the healthcare industry reported the highest number of data

[8] http://blogs.wsj.com/law/2015/12/09/employee-error-leading-cause-of-data-breaches-new-survey-says/.
[9] http://www.acc.com/aboutacc/newsroom/pressreleases/accfoundationstateofcybersecurityreportrelease.cfm

breaches, followed by the insurance, manufacturing, and retail industries. Data breaches in the healthcare industry are particularly worrisome given the likelihood that such breaches would result in HIPAA violations.

iv. **Consequences of Data Breaches**. Data breaches can have numerous consequences, such as timely and expensive efforts remedial efforts, loss of valuable and/or necessary information, and the potential advantage to competitors' access to the information in question. Data breaches can also leave employers liable to those affected by the breach.

EXAMPLE: The data breach Sony Pictures Entertainment Inc. suffered in 2014 prompted affected employees to file a class action against Sony, claiming that Sony was liable for the theft of the employees' personal data in *Corona et al v. Sony Pictures Entertainment Inc*., U.S. District Court, Central District of California, No. 14-09600. After the U.S. District Judge allowed the employees to proceed with their claims that Sony was negligent and violated a California confidentiality law, the parties submitted a proposed settlement in October 2015. Pending court approval, the settlement requires Sony to pay up to $8 million to compensate the individual employees' identify theft losses, the protective measures they were forced to undertake, and their legal fees and costs.

8) Appropriate Response to Threat of Data Breaches.

i. **Train Employees**. Re-evaluating IT departments and updating firewall software are important; but given that employee error is the leading reported cause of data breaches, training is critical to avoiding data breaches and the consequences they entail.

ii. **Purchase Cybersecurity Insurance**.

9) Inappropriate Response to Threat of Data Breaches. Employers must be careful not to overreact to the threat of data breaches or be overzealous in their protection against such unwanted disclosures, because protecting against data breaches may implicate employee privacy and leave employers vulnerable to related employee claims.

10) Florida Statute §501.171, Security of Confidential Personal Information. The statute provides that a "covered entity" must take reasonable measures to protect and secure data in electronic form containing personal information. This may be construed to include an employer's obligation to secure employee personal information.

i. A "covered entity" means a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial

entity that acquires, maintains, stores, or uses personal information, and it includes a governmental entity.

ii. "Personal information" includes an individual's name, social security number, driver's license or ID number, passport or military ID number; financial account information, medical history information; health insurance policy information or identification; username and email address with the password or security question(s) and answer(s).

iii. Covered entities are also required to give notice of security breaches.

DISCLAIMER

The laws and cases referenced in these materials may have changed since the date of publication.

These materials are being made available for informational purposes only and are not to be relied upon as legal advice.

If you have an employment law question,
we urge you to seek legal counsel.