PRIVACY AND SOCIAL MEDIA IN THE WORKPLACE

by

Cynthia N. Sass, Esquire

Sterling Education Services
Employment Law: Beyond the Basics
January 15, 2014

Available Courtesy of:
Law Offices of Cynthia N. Sass, P.A.
601 West Dr. Martin Luther King Jr. Boulevard
Tampa, Florida 33603
(813) 251-5599
www.EmploymentLawTampa.com

PRIVACY AND SOCIAL MEDIA IN THE WORKPLACE[1]

A. BALANCING AN EMPLOYER'S RIGHT TO KNOW VS. EMPLOYEE'S PRIVACY

1. **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:** In its June 17, 2010 decision in *City of Ontario v. Quon*, the United States Supreme Court intentionally refused to address the issue of an employee's right to privacy in employer-issued electronic equipment reasoning that "[a] broad holding concerning employees' privacy expectations vis-à-vis employer-provided technological equipment might have implications for future cases that cannot be predicted." The Court held instead, an employee's expectation of privacy in a workplace communication must be decided on a "case-by-case basis." 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.
2. **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:

[1] The following material is intended to provide information of a general nature concerning the broad topic of employment law issues. The materials included in this paper are distributed by the Law Offices of Cynthia N. Sass, P.A., as a service to clients and other interested individuals. The outline contained herein is provided for informal use only. This material should not be considered legal advice and should not be used as such. Thank you to Yvette D. Everhart, Esquire, of the Law Offices of Cynthia N. Sass, P.A., for her assistance in preparing these materials.

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

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).

3. **Cases Where No Expectation of Privacy Held Because of Employer Policy:**
   - *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 e-mail 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 e-mail where employee handbook explicitly warned of employer's right to monitor files and e-mail).

- *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 e-mail policy prohibited certain uses, the e-mail system belonged to the company, although the company did not intentionally inspect e-mail usage, it might do so where there were business or legal reasons to do so, and the plaintiff assumed her e-mails might be forwarded to others).

4. **No Expectation of Privacy, Even Though Company Expressly Stated They WOULD NOT Monitor Employees' E-Mail:**

   - *Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996) (employee had no reasonable expectation of privacy despite assurances that e-mail sent over the company e-mail system would not be intercepted by management; when employee communicated a comment over e-mail 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).

5. **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").

6. **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 e-mail 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 e-mails).

7. **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 e-mails to her attorney confidential by using her personal, web-based e-mail 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 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 e-mails 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).

8. **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.")

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

1. Privacy Considerations on Wireless Devices

a. Provided by Employer. Privacy considerations will be the same as those discussed in Section A.

1) 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 policy in place.

2) CAUTION: Even when employees use employer devices, an employer reviewing an employee's personal e-mails on the device may violate federal law.

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

b. Provided by Employee.

1) Bring Your Own Devices or "BYOD". Increasing trend of employees using personal devices (i.e. smartphones, tablets, blackberries) to perform work. Sometimes referred to as a dual-use device.

2) Privacy and BYOD:

i. Issue Created. Balancing the employee's privacy versus the employer's interest in protecting its company information, trade

secrets, data, etcetera.

ii. An employee will have a reasonable expectation of privacy in his or her own personal device.

- BYOD is still in its infancy so there is little guidance from the courts in this arena. But as the BYOD trend spreads, there will be a rise in litigation over privacy considerations involving employee personal devices.
- Legal considerations for employer intrusions on personal devices. See Section C regarding federal and state laws regulating same.

3) Examples of where employers were entitled to search employee personal devices.

- *Kamalu v. Walmart*, 2013 WL 4403903 (E.D. Ca. 2013) (employer had the right to go into personal cell phone records of employee claiming national origin, sex, and race discrimination, to support their 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) (personal cell phone was used in plaintiff's work as a sports agent. Employee had limited expectation of privacy concerning his phone records because the phone was a BYOD that was paid for by both the employee and the employer. Although plaintiff received an

employee manual which included the policy on employee's use of employer's equipment, plaintiff did not read the manual nor did he sign an acknowledgement form saying he did read it/would read it).

2. Potential Risks of BYOD:

a. Performance Management. The intermingling of personal and business use on employee devices may affect the productivity and performance of employees.

b. Preservation and Lack of Control over Company Information. Employees using their personal devices make it 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 employee separates from the employer.

c. 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.

d. 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, the 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 2200 patients. The thumb drive was stolen from the employee's car.

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

f. Employee Misconduct. Absent clear and strong BYOD policies, the use of BYODs can also make it a challenge for employers to determine whether employees have misappropriated company information or trade secrets.

3. Tips for an Effective BYOD Policy

a. Have employees who are using their own personal devices to perform work sign confidentiality agreements to protect company information, trade secrets, etcetera, from disclosure to third parties, including their friends and family.

b. Reduce the 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 (i.e. termination, to protect confidential or proprietary information, in the event of a litigation hold) and obtain written consent to monitor the employees' personal device.

c. Create expectations as to behavior by employees while using a dual device, but avoid infringing upon employee freedoms and off-duty conduct.

d. Implement policies and procedures for the return of company information, trade secrets, files on employee personal devices or the policies and procedures for lost or stolen devices.

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

f. 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 to preserve the information on the employee's personal device.

g. Prohibit the intermingling of company and personal information on the device.

    EXAMPLE: Separate e-mail accounts on the device or separate folders or locations for company information versus personal information.

h. When an employee separates, get an agreement to provide access to company information stored on personal devices.

    EXAMPLE: An employer may want to incorporate these types of obligations in employee severance agreements.

To avoid these risks involving BYOD, it may be best for companies to eliminate the use of employee personal devices for work purposes, especially if trying to protect confidential trade secrets, customer information and the like.

C. MONITORING AND CREATING POLICIES REGARDING INTERNET, E-MAIL, TEXTING, AND OTHER ELECTRONIC COMMUNICATIONS

Monitoring social media and other electronic sources in the workplace raises numerous issues:

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

   a. 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 public employee pursuant to his or her official duties.

      1) Social Media Postings Protected Speech.

         - *Bland v. Roberts*, 730 F.3d 368 (4th Cir. 2013) ("Liking" a Facebook® page for a political campaign is a substantive statement and can constitute pure speech as well as symbolic expression protected by 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).

      2) Social Media Postings Not Protected Speech.

         - *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).

3) 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 an 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).

b. 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).

2. **Laws To Be Aware Of.**

a. The Stored Communications Act. The Stored Communications Act, 18 U.S.C. §2701, *et seq*. ("SCA"), prohibits intentionally accessing stored communications without authorization or in excess of authorization which, again, is why a well-drafted communications policy is so important. The SCA

provides for a cause of action to remedy conduct constituting a violation. Those remedies include preliminary and other equitable and declaratory relief as may be appropriate, actual damages suffered by the plaintiff, any profits made by the violator as a result of the violation, punitive damages where appropriate (for willful or intentional violations), a reasonable attorney's fee and other litigation costs reasonably incurred. The SCA also states that in no case shall a person entitled to recover receive less than the sum of $1,000. 18 U.S.C. §2707. In addition, there are possible criminal penalties including a fine and imprisonment for up to 10 years. 18 U.S.C. §2701(b).

1) Accessing Employees' Electronic Communications: Performing searches of employees' e-mail (particularly private e-mail accounts such as an employee's private gmail account whose log-in information may be saved on a company computer) or social media profiles may violate federal law.

   - *Ehling v. Monmouth-Ocean Hospital Service Corp.*, 2013 U.S. Dist. LEXIS 117689, Case No. 2:11-cv-03305 (WJM) (D.N.J. Aug. 20, 2013) (court held that non-public Facebook® wall posts are covered by SCA as they are electronic communication, transmitted by electronic communication services and are in electronic storage but that 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/ECPA where employer allegedly accessed employee's Facebook® images and there was a factual issue as to how the employer accessed or obtained the Facebook® images).

- *Castle Megastore Grp. v. Wilson*, 2013 U.S. Dist. LEXIS 25350 (D. Az. Feb. 25, 2013) (dismissing employer's claim against former employees under the SCA where employer alleged that the employee changed the company's Facebook® password following the termination; the court dismissed the claims because the employer failed to allege that the Facebook® account constituted an electronic communication service under the SCA).
- *Snyder v. Fantasy Interactive, Inc.*, 2012 U.S. Dist. LEXIS 23087 (S.D.N.Y. Feb. 9, 2012) (holding that plaintiff stated a claim for violation of SCA where employer accessed plaintiff's private Skype™ instant messages outside of the office).
- *Maremont v. Susan Fredman Design Grp.*, 2011 U.S. Dist. LEXIS 140446 (N.D. Ill. Dec. 7, 2011) (denying summary judgment on employee's claim for violation of SCA when employer accessed employee's Facebook® and Twitter accounts without permission).
- *Shefts v. Petrakis*, No. 10-cv-1104, 2011 U.S. Dist. LEXIS *16 (C.D. Ill. Nov. 29, 2011) (stating that 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) (finding that plaintiff sufficiently pled claim under SCA where defendant allegedly used keylogger software to access plaintiff's e-mail and financial accounts).
- *Pietrylo v. Hillstone Restaurant Group*, 2008 WL 6085437 (D.N.J. 2008) (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." Pietrylo 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 plaintiffs claimed that Hillstone violated the SCA when it accessed the group without authorization and the jury agreed).

2) Pre-Employment Research: Further, when performing pre-employment searches of 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.

- *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 883-84 (9th Cir. 2002) While 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.

b. The Computer Fraud and Abuse Act. A number of cases have involved employers alleging violations of the Computer Fraud and Abuse Act, 18 U.S.C. §1030 ("CFAA"). The CFAA prohibits the unauthorized access of a computer (or exceeding authorized access of a computer) and obtaining information. The problem often arises when departing employees attempt to gain an advantage by stealing information from their employer prior to their departure. The statute focuses on whether the employee's accessing of the company computer was without authorization or exceeded any authorization which was granted. There is disagreement among the circuits as to when an employee acts with the requisite authorization. The CFAA provides both criminal penalties including fines and imprisonment for up to 10 years (18 U.S.C. §1030(c)) and a civil cause of action for certain violations of the CFAA where compensatory damages and other injunctive or equitable relief may be granted. 18 U.S.C. §1030(g).

1) Violation of CFAA:

- *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010) (Court adopted a broad construction of the CFAA, that "without authorization" and/or "exceeds authorized access" includes employee misusing employer information that he or she is otherwise permitted to access. Employee found guilty for accessing information that was not in the furtherance of his job duties).
- *Ryan, LLC v. Evans*, 2012 U.S. Dist. LEXIS 59692 (M.D. Fla., Apr. 30, 2012) (relying on *Rodriguez* declined to follow magistrate's finding no unauthorized access where employees had unfettered access to employer data, information and computers and the right to add to, delete from and upload or download information).
- *See also Eagle v. Morgan*, 2012 U.S. Dist. LEXIS 143614 (E.D. Pa. Oct. 4, 2012) (employer's access to a former employee's LinkedIn® site that was associated with the employer may have violated the CFAA, but summary judgment granted for the defendant because the plaintiff could not prove a cognizable loss as a result of the access).

2) No Violation of CFAA:

- *Keen v. Bovie Med. Corp.*, 2013 U.S. Dist. LEXIS 64999 (M.D. Fla. May 7, 2013) (employee's access to employer-owned laptop was authorized and not violative of CFAA).

- *Trademotion, LLC v. Marketcliq, Inc.*, 857 F. Supp. 2d 1285 (M.D. Fla. Feb. 14, 2012) (because an employee had been granted full administrative access, a claim could not be brought under the CFAA regardless of how access was used).
- *Lee v. PMSI, Inc*., 2011 U.S. Dist. LEXIS 52828 (M.D. Fla. May 6, 2011) (no violation of CFAA where employee accessed personal websites from employer computer while working; further, employer could not show that employee was without authorization to access work computer).
- *Clarity Servs. v. Barney*, 698 F. Supp. 2d 1309 (M.D. Fla. 2010) (CFAA claim failed because employee had authorized access to computer although used authorization to access an e-mail from the employer's e-mail account after his termination and deleted customer information on employer's laptop).
- *See also Power Equip. Maint., Inc. v. Airco Power Servs.*, 2013 U.S. Dist. LEXIS 91484 (S.D. Ga. June 28, 2013) (cannot state a claim under the CFAA where employee had authorized access, properly accesses information, and merely uses it to employer's detriment).

c. The Electronic Communications Privacy Act. Title I of the Electronic Communications Privacy Act, 18 U.S.C. §2510, *et seq.*, a/k/a the Federal Wiretap Act ("ECPA") regulates the search and seizure of electronic communications while they are in transit. It provides civil and criminal

penalties for 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. However, under the ECPA, consent to the interception by one party to the communication is a defense to a violation. The ECPA provides for separate causes of action both by private individuals and by the government.

- In a private cause of action under the ECPA, a plaintiff may recover preliminary and other equitable or declaratory relief as may be appropriate, declaratory damages, punitive damages where appropriate, reasonable attorney's fees and other litigation costs reasonably incurred. 18 U.S.C. §2520.
- Notably, the ECPA provides that the plaintiff will receive at a minimum $10,000, regardless of a showing of any actual damages. 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).
- Finally, the ECPA provides for criminal penalties including a fine and imprisonment for up to five years. 18 U.S.C. §2511(4).

1) Interception:
    - *Shefts v. Petrakis*, 2012 U.S. Dist. LEXIS 130542 (C.D. Ill. Sept. 12, 2012) (in an action between owners of a telecommunications company, co-owners accessing Yahoo!®-based e-mails as well as a

screen-capture software that took images of plaintiff's computer activities constituted interceptions in violation of the ECPA).

- *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 e-mail account so that any e-mail that was sent to the employee's supervisor was also forwarded to him).

2) No Interception:

- *See Ehling v. Monmouth-Ocean Hosp. Serv.*, 872 F. Supp. 2d 369 (D.N.J. May 30, 2012) (dismissing claim under analogous state wiretap act against an employer who accessed an employee's private Facebook® page via another employee's account because the posting accessed was in "post-transmission storage").
- *See Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 883-84 (9th Cir. 2002) (the airline pilot sued the 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).

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

1) Consumer Report. The phrase "consumer report" 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.**

2) 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).

3) Employment Purposes. The definition of "employment purposes" is a report used for the purpose of evaluating a consumer for employment, promotion, reassignment or retention as an employee.

4) 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.

5) 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).

6) 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.

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

8) 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.

9) 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.[1]
- 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.

e. 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

[1] *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).

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 e-mails, chat conversations and instant messages).

3. **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:

   a. be motivated by a legitimate work-related purpose; and

   b. not be excessively intrusive in light of the justification.

   - *City of Ontario v. Quon*, 130 S. Ct. 2619, 2628 (2010). In *Quon*, 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.

- 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. AGO opinion 2009-19.

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.

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

   a. 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.

   b. 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.

   c. 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 pruposes.**

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

   e. 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").

f. 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, etc.).

g. 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.)

h. Prohibitions on Actions. Prohibit the forwarding of any e-mails or other documents from company servers to employees' personal e-mail accounts or computers, unless employees are using BYOD devices. See Section B. Be clear that any communication which occurs on company-provided electronic systems is company property.

i. 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.

j. 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, etc.). 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.

k. 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, etc., they will better remember the policy before engaging in such behavior.

l. 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.

m. 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.

n. 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 what is permissible and what is not, in addition to providing a possible basis for discrimination.

o. Former Employees. Ensure that all comments, recommendations, criticisms etc. 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.

p. 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.

q. Tracking Electronic Use. Be clear that the company reserves the right to track employees via the Internet, e-mail and mobile phone use.

r. 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.

s. 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.

t. 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 e-mail and Internet use, employers must be careful not to violate Section 7 by limiting employees' ability to openly discuss work-related concerns. See Section F.

5. **Common Law Invasion of Privacy Considerations**. Florida recognizes three common law invasion of privacy claims: 1) intrusion upon seclusion; 2) appropriation of likeness; and 3) public disclosure of private facts.

a. Intrusion Upon Seclusion 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).

b. Public Disclosure of Private Facts 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).

c. Appropriation of Likeness 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.

6. 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).

7. Other Jurisdiction Case Law: Claim for Invasion of Privacy.

Eagle v. Morgan, 2013 U.S. Dist. LEXIS 34220 (E.D. Pa. Mar. 12, 2013) (finding that employer misappropriated former employee's name for its "own use or benefit the reputation, prestige, social or commercial standing, public interest or other values of plaintiff's name" when it maintained a LinkedIn® home page under a web address containing the plaintiff's name).

D. USE OF SOCIAL NETWORKING SITES IN THE EMPLOYMENT CONTEXT: RISKS, BEST PRACTICES, AND POLICIES

1. What Are the Benefits of Using Social Media and What Are the Risks and Practices to Minimize Those Risks?

a. Benefits:

1) Recruiting. Nearly three out of four hiring managers and recruiters check candidates' social media profiles.[1]

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 that an employee was really at the beach or an amusement park on a day they called in sick or 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").

EXAMPLE: When employees who drive as part of their duties, the use of GPS to track such employees' movements can be key evidence to establish the whereabouts of a party which may be determinative of factual disputes.

[1] Jobvite, *Jobvite Social Recruiting Survey Finds Over 90% of Employers Will Use Social Recruiting in 2012* (July 9, 2012), available at http://recruiting.jobvite.com/company/press-release/2012/jobvite-social-recruiting-survey-2012/

- *Frew v. Tolt Techs. Serv. Group, LLC*, 2010 U.S. Dist. LEXIS 11991 (M.D. Fla. Feb. 10, 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).
- *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).

4) Investigate Abuse of FMLA Leave.
   - *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. The law is still developing on whether connecting with contacts on social media violates restrictive covenants:

i. Connecting with Contacts May Violate Restrictive Covenants.

- *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).
- *But see, 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).

ii. Updating or Posting on Social Media May Violate Restrictive Covenants.

- *See 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).
- *Compare 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).

7) Other 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 surreptitiously determine what communications employees are having. Additionally, certain key logging programs will 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, while used by some employers, are legally questionable to say the least. Presently, courts are reluctant to find that use of keylogging software violates the ECPA:

- *United States v. Barrington*, 648 F.3d 1178 (11th Cir. Fla. 2011) (use of keylogging software did not violate ECPA because although keylogged data was accessed remotely, this particular keylogging software did not contemporaneously capture and transmit keylogged 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 may constitute violation under the SCA).

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, or even implant them. RFID tags are most commonly attached to ID badges and security cards to grant access to secure areas. However, the tags can also be monitored 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, etc.

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. As employers begin to move to these types of technologies, privacy concerns will still be an issue. Not only will biometrics in the workplace raise privacy concerns, but the use may also give rise to discrimination claims.

EXAMPLE: On September 25, 2013, the EEOC filed suit against Consol Energy and Consolidation Coal Company for religious discrimination by requiring an employee to use biometric hand scanner to trace employee hours and attendance. The employee repeatedly objected to the use of biometric scanning as the use violated his religious beliefs (Evangelical Christian). The employer refused to provide the employee with a religious accommodation, which ultimately resulted in the employee being forced to retire. *See EEOC v. CONSOL Energy, Inc. and Consolidation Coal Company*, Case No. 1:13-cv-00215-IMK) (N.D. W. Va.).

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.

b. Risks:

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.

- *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).[2]

[2] 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).

- *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.[3]

- *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

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

the basis for discipline as some conduct may be protected activity as discussed below in Section F).

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) 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.

   i. 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).

ii. Federal Trade Commission Guidelines, 16 C.F.R. Part 255. Employers may face liability for employees commenting on their employer's services or products on blogs or social networking sites if the employment relationship is not disclosed.

6) Legal Considerations.

i. Regulations. The laws regulating it (see also Section C above).

ii. Potential Violation of the Fair Credit Reporting Act. See Section C above.

iii. Violations of the Fair Labor Standards Act ("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.

iv. 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 e-mailing 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.)

v. State Laws that Impact the Use of Social Media in Hiring. Although Florida has not yet followed the trend, other state lawmakers began to introduce 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, *Employer Access to Social Media Usernames and Passwords 2013*, available at: http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords-2013.aspx.

c. Minimizing 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 C.

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, etc.
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.

- *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.

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 D.3.

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.

    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.

2. Ensure Compliance with Record Retention Requirements.

a. 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.)

b. 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.

c. 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.

E. OFF-THE-JOB BEHAVIOR, E.G., BLOGGING AND DATING

1. **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.

   a. Cases on Employer Liability for Off-Duty Electronic Communications.

      1) Facebook®.

         - *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.)

2) 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.)

3) 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).

4) 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, etc. There was also a message board where co-workers posted derogatory and harassing messages about Blakely. 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).

b. Unemployment. In July 2011, Florida amended the unemployment law definition of misconduct to disqualify applicants from receiving unemployment benefits for conduct which could 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…").

c. 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.

F. THE NLRB AND SOCIAL MEDIA

1. **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.**

   a. Definition of "Employee" Under the NLRA. 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.

   b. Definition of "Employer" Under the NLRA. 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.

c. 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.[1] When an employee suffers an adverse employment action as a result 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

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

for language posted on the Internet.

d. 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.

e. Recent Case Trends Under the NLRA – Decisions by the NLRB.

- *Richmond District Neighborhood Center*, Case No. 20-CA-091748 (Nov. 2013) (NLRB held that employees' Facebook® postings were concerted, but not protected activities. The two employees at issue received rehire letters following their summer at the center. Prior to leaving, there was a group meeting where the employees engaged in concerted protected activities and complained about the working environment. Months later, these two employees engaged in a conversation on Facebook® about returning to the camp, doing whatever activities they wanted with the kids and letting the center figure out how to fund it. After a Facebook® friend who worked for the center saw the posts, the center rescinded their re-hire

offers. The employer argued that it had a legitimate reason for rescinding the job offers because the employees' comments "jeopardized the program's funding and safety of the youth it serves." The NLRB agreed that the employees discussions on Facebook®, while concerted were not protected).

- *Pflantzer v. New York Party Shuttle, LLC*, 359 NLRB No. 112, Case No. 02-CA-073340 (May 2013) (NLRB held that employer violated NLRA by failing to give an employee work assignments because the employee publicized his union activities and concerted activity in e-mail communications and Facebook® posts).
- *But see Tasker Healthcare Group*, Advice Memo, Case No. 04-CA-094222 (May 2013) (advising that the employer did not violate the NLRA for discharging an employee who participated in a Facebook® private group message because the employee's comments and personal gripes about the employer were not protected activity).
- *Design Technology Group, LLC (Bettie Page Clothing) v. Morris*, 359 NLRB No. 96, Case No. 20-CA-035511 (Apr. 2013) (NLRB held that employer violated the NLRA by terminating employees for engaging in concerted protected activities that included postings on Facebook® complaining about treatment by their supervisor).
- *DirecTV*, 359 NLRB No. 54, Case No. 21-CA-039546 (Jan. 2013) (finding that DirecTV's intranet policy on the use of social media was

unlawful because it prohibited the disclosure of information from employee records including information regarding wages, discipline and performance ratings).

- *Hispanics United of Buffalo, Inc.*, 359 NLRB No. 37, Case No. 03-CA-027872 (Dec. 2012) (NLRB found that employer violated NLRA by discharging employees who engaged in concerted activity in Facebook® posts. Specifically, an employee posted a message on her Facebook® page asking her co-workers how they felt about another employee's criticism that the employees do not work hard enough for the clients and other employees responded to the post, defended themselves and criticized the working conditions).
- *EchoStar Techs., LLC*, Case No. 27-CA-066726 (Sept. 2012), (*aff'd* N.L.R.B., Nov. 1, 2012) (ALJ found that employer's social media policy prohibiting employees from making "disparaging or defamatory" comments chilled an employee's Section 7 rights. The NLRB further held that the savings clauses provided in the handbook did not save the rule from violating Section 7.)
- *Knauz BMW*, 358 NLRB No. 164, Case No. 13-CA-046452 (Sept. 2012) (NLRB noted that charging party's comments on Facebook® that the decision by the employer to serve potential clients hot dogs was "cheap" and may negatively affect his earnings would potentially constitute concerted protected activity; however, the NLRB found that the charging

party's termination was lawful based on other Facebook® posts that were not concerted activity. Significantly, the NLRB held that certain language in the employer's handbook violated the NLRA).

- *Costco Wholesale Corporation*, 358 NLRB No. 106, Case No. 34-CA-012421 (Sept. 2012) (finding that Costco violated the NLRA by maintaining a rule that prohibited employees from electronically posting statements that harm the company's reputation or defame the company).

f. On the Horizon. Currently, pending before the NLRB is whether "liking" a Facebook® post constitutes protected activity under the NLRA. *See Triple Play Sports Bar*, Case No. 34-CA-12915. In *Triple Play Sports Bar*, the ALJ found that a charging party's "liking" a Facebook® status that constituted concerted activity was also covered protected activity under the NLRA. Triple Play Sports Bar appealed the ALJ's decision and the NLRB has yet to issue a decision.

g. Other Cases. The Acting General Counsel for the NLRB issued reports containing other cases presenting emerging social media issues on August 18, 2011, January 24, 2012, and May 30, 2012. The complete reports can be found on the NLRB's website at http://www.nlrb.gov/publications/operations-management-memos (OM 11-74, OM 12-31, and OM 12-59 respectively). The reports analyzed:

- Whether employers' social media policies were unlawful restrictions of employees' NLRA rights under Sections 7 and 8(a)(1); and

- Whether employees' conduct constituted protected activity under the NLRA.

h. The Overarching Themes of the Listed Decisions Were:

- Overly broad social media policies that create a chilling effect because employees do not know what is and is not prohibited, are less likely to be enforced; and
- There is a direct correlation between the degree to which the employee's activity relates to the workplace and involves other employees, and the likelihood the employee's social media activity will be considered concerted activity.

i. Examples of Employer Policies that were Unlawfully Overbroad[2]:

1) Employer's rule prohibiting employees from "[m]aking disparaging comments about the company through any media, including online blogs, other electronic media or through the media" was unlawful, as it "would reasonably be construed to restrict Section 7 activity." Notably, the NLRB pointed out that the policy did not contain limiting language (sometimes referred to as a "savings clause") that would clarify to employees that the rule does not restrict their Section 7 rights.

2) Employer's rule prohibiting employees from identifying themselves as the employer's employees in social media forums unless discussing the terms and conditions of their employment in an "appropriate manner" was

[2] Although citations would be helpful for these examples, the NLRB did not provide any.

unlawful under the NLRA. Notably, the employer's policy did include a savings clause stating that the rule was in no way meant to restrict an employee's right to participate in concerted activity. However, the NLRB held that despite the limiting language, employees had no way of knowing which discussions the employer considered "appropriate." (Also may violate FTC regulations requiring a promoter of a company's products and services to identify their relationship to the company when posting anything about the company's products or services in online posts, such as online reviews, testimonials, including those on social media sites. *See 16 C.F.R. Part 255*)

3) Employer's rule that prohibited "disrespectful conduct" and "inappropriate conversations" was unlawfully overbroad under the NLRA because it could be reasonably interpreted to preclude Section 7 activity.

4) Employer's social media policy prohibiting employees from "using social media to engage in unprofessional communication that could negatively impact the employer's reputation or interfere with the employer's mission or unprofessional/inappropriate communication regarding members of the employer's community" was unlawful under Section 8(a)(1) because it could reasonably be construed to chill employees in the exercise of their Section 7 rights.

5) Employer's rule prohibiting employees from "disclosing or communicating information of a confidential, sensitive, or non-public

nature concerning the company on or through company property to anyone outside the company without prior approval of senior management or the law department" was unlawfully overbroad under the NLRA. Employees have a right to discuss terms and conditions of their employment with co-workers as well as non-co-workers. Further, it is unlawful to require employees to obtain prior approval from the employer before engaging in protected activity.

6) Employer's rule prohibiting the use of the company's name or service marks outside the course of business without the prior approval of the legal department was unlawfully overbroad under the NLRA.

7) Employer's rule prohibiting employees from publishing any representation about the company, including statements to the media, media advertisements, electronic bulletin boards, weblogs, and voicemail, without prior approval by senior management and the legal department was unlawfully overbroad under the NLRA.

8) Employer's rule requiring social networking site communications be made in an "honest, professional, and appropriate manner, without defamatory or inflammatory comments regarding the employer and its subsidiaries, and their shareholders, officers, employees, customers, suppliers, contractors, and patients" was unlawful in that employees could not know which communications the employer would deem "professional" or "appropriate."

9) Employer's rule that employees needed the approval of the company to identify themselves as employees of the company and that those employees who had identified themselves as such on social media sites must expressly state that their comments are their personal opinions and do not necessarily reflect the employer's opinions was unlawful. Social media pages serve as an important way for employees to find and connect with each other; therefore, limiting their ability to identify each other is harmful to the exercise of their rights. Additionally, making employees state that the opinion is their own each time they discuss the terms and conditions of their employment would be overly burdensome.

j. Whether Employees' Conduct was Concerted Activity Under the NLRA:

1) Employee engaged in concerted activity where she posted profane messages on her Facebook® page saying she disagreed with the employer's decision to demote her. Employee's co-workers who were also her Facebook® friends commented on the posts, agreeing with the employee. Others suggested taking collective action in the form of a class action lawsuit. The NLRB's definition of concerted activity encompasses an employee's initiation of group action through the discussion of complaints with fellow employees.

2) Employee's termination was made pursuant to an unlawfully overbroad non-disparagement rule and therefore also violated Section 8(a)(1). Employee was notified that she was being terminated due to her comments

on Facebook®, and the employer showed her a copy of her Facebook® wall. Discipline imposed pursuant to an unlawfully overbroad rule violates the NLRA in those situations in which an employee violated the rule by:

- Engaging in protected conduct, or
- Engaging in conduct that otherwise implicates the concerns underlying Section 7 of the NLRA.

However, an employer will not be liable for discipline imposed pursuant to an overbroad rule if it can establish that the employee's conduct actually interfered with the employee's own work or that of other employees or otherwise actually interfered with the employer's operations, and that interference was the reason for the discipline.

3) Employee did not engage in concerted activity when, after being reprimanded, she posted "[expletive][employer name]" on her Facebook® wall. Although at least one of her co-workers "liked" the post, it was "merely an expression of an individual gripe." Employee had no particular audience in mind, used no language attempting to induce others to engage in group action, and the post did not result from previous conversations with co-workers about the terms and conditions of employment.