EMPLOYEE DOCUMENTS, DISCIPLINE AND DISCHARGE

by

Cynthia N. Sass, Esquire

National Business Institute
Live Webinar
July 2013

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

EMPLOYEE DOCUMENTS, DISCIPLINE AND DISCHARGE[1]

Cynthia N. Sass, Esquire
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

I. RECRUITMENT/HIRING DOCUMENTS.

A. The Importance of an Accurate Job Description.

1. Management Tool. An accurate job description is essential in assisting employers in identifying duties that are required for a job which in turn identifies skills needed as well as evaluating staffing needs.
   - Update and review job descriptions for accuracy yearly.
   - Get input from the employees as to duties and responsibilities.
   - Get input from supervisors as to duties and responsibilities.
2. Documentation. An accurate job description is one piece of evidence used to evaluate compliance with employment laws. For example:
   a. **Fair Labor Standards Act of 1938, 29 U.S.C. §201, *et. seq.* (FLSA)**. Job descriptions can be determinative in determining exempt or non-exempt status from the minimum wage and/or overtime provisions of the FLSA.

[1] The following material is intended to provide information of a general nature concerning the broad topic of employment law. The materials included in this paper are distributed by the Law Offices of Cynthia N. Sass, P.A., as a service to interested individuals. The outlines contained herein are provided for informal use only. This material should not be considered legal advice and should not be used as such. The Law Offices of Cynthia N. Sass, P.A. would also like to thank Professor Robert Sprague of the University of Wyoming for his contributions to the off-duty conduct statutes and state legislation regarding access to social media portions of this outline. Thank you to Yvette D. Everhart, Esquire, of the Law Offices of Cynthia N. Sass, P.A. for her assistance in preparing these materials.

b. **Equal Pay Act of 1963, 29 U.S.C. §206(d) (EPA)**. Job descriptions can be determinative in equal wage comparisons to ensure that males and females performing the same or similar position are equally compensated.

c. **Americans with Disabilities Act of 1990, as amended by the ADAAA, 42 U.S.C. §12101, *et seq.* (ADA)**. Job descriptions can be determinative as to whether a duty is an essential function of a job which in turn assists in determining whether a person with a disability is qualified for the position. In addition, a job description assists in the determination of whether providing an accommodation is appropriate.

3. Case Law. Inaccurate job descriptions found to be probative evidence of discrimination:

   a. *Kimble v. Wasylyshyn*, 439 Fed. Appx. 492 (6th Cir. 2011) (in a race discrimination case, finding that a reasonable jury could conclude that selection criteria not included in the position description was used to advance a specific candidate over another candidate in a protected class).

   b. *Duncan v. Fleetwood Motor Homes of Indiana*, 518 F.3d 486 (7th Cir. 2008) (in disability and age discrimination cases, finding that essential functions of the job listed in the paper job description did not match the actual job requirements. It found that removal of employee from position because employee could not perform requirements in the paper job description to be false and not a legitimate reason).

   c. *Courtney v. Biosound, Inc.*, 42 F.3d 414, 421 (7th Cir. 1994) (in age discrimination case, denying summary judgment for employer finding that a reasonable jury could draw an inference that an employer's reasons for non-selection of the plaintiff where there was a disparity between what the employer claimed to be essential elements of the position, which were not listed in the position description, and what the employee actually performed).

d. *Gaworski v. ITT Commercial Fin. Corp.*, 17 F.3d 1104 (8th Cir. 1994) (age discrimination case, finding employer's stated reason for retaining younger employee due to greater computer skills over older employee was not reasonable where the job description lacked a computer skills requirement to do the job and younger employee was applying computer skills less than the older terminated employee).

4. Elements. A job description should contain the following elements:
   - Essential duties and responsibilities of the position – include any physical requirements of the job and not the physical requirements of an employee.
   - Date the job description was updated.
   - FLSA exemption status (i.e. exempt, non-exempt).
   - Requirements and/or criteria to qualify for the job, such as educational requirements, trainings, certifications, etcetera.
   - Gender neutral description.
   - To ensure no discriminatory job requirements, avoid adjectives referring to candidates or employees such as:
     - "young,"
     - "healthy," or
     - "single;"
   - Have employee sign and date job description to verify it is accurate.

B. Internal Job Opportunity Notices.

1. Requirements. Generally, there is no requirement that an employer post job vacancies, either internally or externally. However, job postings may be required by the following:
   a. Collective bargaining agreement;
   b. Government contract;
   c. If governmental agency, check the rules and regulations of the agency;
   d. Specific state or local law; and/or
   e. Policy of employer.

2. Elements. Job opportunity notices should contain the same elements as noted for job descriptions.
3. Internal Posting.
    a. **Benefits**. The benefits of posting internal job opportunities are:
        - Motivation of current employees; and
        - Good resource for filling positions.
    b. **Risks**. The downside of posting internally is that if it is not done properly, it may set up expectations that internal candidates have priority for the job over outside candidates. If posting an internal job, an employer needs to:
        - State in its policy that an internal posting of positions is NOT required, but that employees are still encouraged to apply for any available positions.
        - Indicate that current employees will NOT be given preference over external candidates, and all candidates are considered equally.
        - Consistently follow its job posting policies to avoid legal claims for discrimination, etcetera.
        - Make sure it is accurate for the same reasons as the need for accurate job descriptions discussed above, as inaccurate job postings could be probative of discrimination.
4. Case Law. Departures from the employer's policies can be probative of discrimination:
    - *Long v. Teachers' Ret. Sys. of Ill.*, 585 F.3d 344 (7th Cir. 2009) ("An employer's departure from its own employment policies can constitute circumstantial evidence of discrimination."); *see also Rudin v. Lincoln Cmty. Coll.*, 420 F.3d 712, 723 (7th Cir. 2005) (departures from stated hiring policies probative of discrimination).
    - *Stern v. Trustees of Columbia University in City of New York*, 131 F.3d 305, 313 (2d Cir. 1997) ("[D]epartures from procedural regularity" can

create an inference of discriminatory intent, sufficient to establish a prima facie case.).

- *Morrison v. Booth*, 763 F.2d 1366 (11th Cir. 1985) ("Departures from normal procedures may be suggestive of discrimination.").

C. The Job Offer Letter. The purpose of the offer letter is to outline the terms and conditions of the employment position being offered.

1. Creating Unintentional Contract Rights. Language in an offer letter can create contract rights that were unintended, such as changing an employment-at-will position to guaranteed employment, termination for just cause.

   a. **General Rule**: In most states, an employee is employed at-will, which means that an individual is employed for an indefinite duration with an employer and can be terminated for any (legal) reason or no reason at all.

   b. **Changing the At-Will Status**. An improperly worded offer letter can alter the employee at-will status IF:

      - The offer letter contains definite terms of employment, such as definite length or period of employment.
        - *Iniguez v. Am. Hotel Register Co.*, 820 So. 2d 953 (Fla. 3d DCA 2002) ("when a contract for employment provides for a definite duration, the employment contract is enforceable"); *see also Watson v. Champion Computer Corp.*, 2000 U.S. Dist. LEXIS 17086 (N.D. Ill. Nov. 22, 2000) (denying summary judgment as to whether offer letter constituted offer for definite term).
      - The employer gives assurances of continued employment, it can sometimes alter employment status in states that recognize *implied in fact* contracts, such as California.
        - *See Foley v. Interactive Data Corp.*, 47 Cal. 3d 654 (1988) (outlining the factors looked at to show an implied-in-fact contract).

c. **Create Contractual Obligations to Compensation or Other Benefits**. Language in an offer letter which sets forth guaranteed compensation and bonuses versus discretionary compensation can create a contract to pay, rather than just an expectation of payment.

- For example, in some states, where the offer letter provides for certain compensation or benefits, such as commissions, these terms may be binding upon the employer even if it does not alter the employment at-will status. *See* *J.R.D. Mgt. Corp. v. Dulin*, 883 So.2d 314 (Fla. 4th DCA 2004) ("It is only an action for breach of *employment* that is barred when the contact of employment is terminable at will; other contractual provisions may not be affected by the at will employment rule.")

2. Job Pre-Requisites.

a. **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.

i. 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.**

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

iii. 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.

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*. You should receive this summary from the consumer reporting agency that gave you the report or you can obtain it 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 You Take an 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.

b. **Drug Testing Concerns**.

i. ADA. Pre-employment drug screens are permitted under the ADA.

ii. Condition of Employment. Give notice to an applicant or employee if he or she will need to submit to a drug screen as a condition of being offered employment.

iii. State Drug-Testing Statutes. In states that have drug-testing statutes, employers should ensure that they are in compliance with those statutes. For example, in Florida, the Drug-Free Workplace Act (Florida Statute §440.102) is not mandatory, but if an employer implements and follows Florida's Drug-Free Workplace Act, the employer has certain obligations, such as:

- Giving written notice of the drug-free policy outlining the expectations, when drug tests can be requested, drugs that will be tested for, consequences for refusing, rights to review of "positive" results, lists of medications that may alter the test results; and

- Allowing a job applicant that receives a positive drug test to contest or explain the results with a medical reviewer within five working days after receiving the positive result.

c. **Physical Agility Test**.

i. ADA. A physical agility test or physical fitness test is permitted under the ADA so long as it is job-related and consistent with business necessity.

ii. Notice. Inform the applicant in the offer letter whether he or she will be required to submit to a physical agility or physical fitness test.

d. **Medical Examinations**.

i. BEFORE a Job Offer is Made.

- Employers should NOT require a medical examination or even ask questions about potential disabilities and/or physical restrictions to perform a job prior to an offer of employment being made to an applicant.
- Employers should check their job applications (both electronic and paper formats) to ensure that there are no questions that may potentially reveal confidential medical information of the applicant. 29 C.F.R. §1630.13(a)-(b).
- If the applicant has an obvious disability, the employer is not prohibited from inquiring how the individual will perform particular essential job functions. 29 C.F.R. §1630.14(a).

ii. AFTER Conditional Job Offer is Made.

- Once an employer gives the employee a conditional job offer, an employer may inquire into disability and/or medical impairments, so long as it does so for all new employees. 29 C.F.R. §1630.14(b).
- However, an employer can only deny an employee a job based on the inquiry if the denial is job related and/or the employer can

show the denial was consistent with business necessity. 29 C.F.R. §1630.14(b)(3).

- If an employer is going to require a medical examination, it is advised that the employer make the medical examination the last step in the hiring process. This would mean extending the employment offer after the applicant has met all job criteria, except the medical examination, and notifying the employee that the job offer is contingent upon the passing of a medical examination or questionnaire.
- **Genetic Information Nondiscrimination Act of 2008, 42 U.S.C. §2000ff, *et seq.* (GINA) Considerations**. Post-offer, pre-employment medical exams of applicants that request family medical history may violate GINA. [*SEE* GINA COMPLIANCE, SECTION E.1(b)(ii) – CHECKLIST FOR A LEGAL HIRE BELOW]

iii. AFTER Employment has Started.

- The EEOC regulations make it clear that an employer can require an employee to submit to a medical examination after the start of employment, if the employer can show the medical examination is job related and consistent with business necessity. 29 C.F.R. §1630.14(c).
- Examples of when employers have required an employee to submit to a medical examination include:
  - To determine if an employee is a direct threat to the health and safety of themselves or other employees in the workplace, 29 C.F.R. §1630.15(b)(2);
  - To determine if an employee is unable to perform the essential job functions because of a medical condition (this inquiry must be made based on a reasonable belief that the employee cannot perform the essential functions), 29 C.F.R. §1630.14(c); or

- Where an employee has requested accommodations and the need for the accommodation is not obvious.

- **GINA Considerations**. Employment medical exams of employees that request family medical history may violate GINA.

3. Terms. Important terms to include in an offer letter are:
   a. A statement that the employment is at-will, a disclaimer that the offer letter is NOT intended to create an employment contract and that the terms and conditions of employment are subject to change at the sole discretion of the employer.
   b. Compensation and whether it is discretionary.
   c. Moving expenses and whether they must be refunded if employee leaves.
   d. The date employment will commence.
   e. Whether the employee will be required to sign a non-compete or other type of agreement as a condition of employment.
   f. A statement that the employee must comply with all policies of the employer.
   g. Whether the employment is conditioned on completion of certain mandatory job pre-requisites, such as drug screen or physical agility tests.
   h. Address social media and expectations as to ownership of social media sites if used for work purposes and who owns the content and contact lists before employee begins working.
      - Depending on the state, however, use caution when requiring social media information regarding a prospective employee's personal social media accounts. [*SEE* STATE LAWS THAT IMPACT THE USE OF SOCIAL MEDIA IN HIRING, SECTION F.5 – USE OF SOCIAL MEDIA IN THE HIRING PROCESS BELOW]
4. Record Retention Requirements.
   a. **Federal Requirements**. Remain unchanged even with the new advent of social media and on-line recruiting.

i. 29 C.F.R. §1602.12. This regulation governs Title VII of the Civil Rights Act of 1964, 42 U.S.C. §2000e, *et. seq.* (Title VII), the ADA, and GINA.

- Employers generally need to retain records that (a) are necessary for the effective operation of the EEO-1 reporting system or of any special or supplemental reporting system as described above; or (b) are further required to accomplish the purposes of Title VII, the ADA, or GINA.
- When employers do keep records, 29 C.F.R. §1602.14 requires employer to retain the following:
  - One year from date of making record or the personnel action involved, whichever occurs later – any personnel or employment record made or kept by an employer (including but not necessarily limited to requests for reasonable accommodation, application forms submitted by applicants and other records having to do with hiring, promotion, demotion, transfer, lay-off or termination, rates of pay or other terms of compensation, and selection for training or apprenticeship). In the case of involuntary termination of an employee, the personnel records of the individual terminated shall be kept for a period of one year from the date of termination.
  - All personnel records relevant to the EEOC charge or action from when charge is filed until final disposition of the charge or the action – where a charge of discrimination has been filed with the EEOC, or an action brought by the Commission or the Attorney General, against an employer under Title VII, the ADA, or GINA.

ii. 29 C.F.R. §1627.3. This regulation governs the Age Discrimination in Employment Act of 1967, 29 U.S.C. §621, *et seq.* (ADEA) and sets forth that:

- For a period of three years, employers are required to keep payroll records (or the equivalent showing name, rate of pay, occupation, etc.);
- For a period of one year from the date of the personnel action, every employer who, in the regular course of his business, makes, obtains, or uses, any personnel or employment records related to the following, shall, retain:
  - Job applications, resumes, or any other form of employment inquiry whenever submitted to the employer in response to his advertisement or other notice of existing or anticipated job openings, including records pertaining to the failure or refusal to hire any individual;
  - Promotion, demotion, transfer, selection for training, layoff, recall, or discharge of any employee;
  - Job orders submitted by the employer to an employment agency or labor organization for recruitment of personnel for job openings;
  - Test papers completed by applicants or candidates for any position which disclose the results of any employer-administered aptitude or other employment test considered by the employer in connection with any personnel action;
  - The results of any physical examination where such examination is considered by the employer in connection with any personnel action; and

- Any advertisements or notices to the public or to employees relating to job openings, promotions, training programs, or opportunities for overtime work.

- For a period of one year after termination, records of any employee benefit plans (i.e. pension plans or insurance plans), as well as seniority systems or merit systems, in writing for the period in which the plans are in effect and for at least one year after the termination of the plan.

iii. FLSA. Every covered employer must keep certain records for all non-exempt employees.

- **Enterprise Coverage**.
  - Employers who have annual dollar volume of sales or receipts in the amount of $500,000 or more and at least two employees who are engaged in commerce, or the handling, selling or otherwise working on goods or materials that have been moved in or produced for commerce by any person;
  - Hospitals or institutions engaged in the care of the sick, aged and the mentally ill or mentally handicapped;
  - Schools, including pre-schools, elementary, secondary and institutions of higher learning;
  - Federal and local government agencies, but NOT the State; and
- **Individual Coverage**.
  - Employees who on an individual basis are engaged in handling or producing goods for interstate commerce, including using of instrumentalities of interstate commerce.
- **Not Covered**.
  - Independent contractors;
  - Trainees; or
  - Volunteers.

- **List of Records Employers MUST Maintain**.
  - Employee's name and social security number;
  - Address;
  - Birthdate, if under 19 years of age;
  - Sex and occupation;
  - Time and day of week showing when work week begins;
  - Hours worked each day;
  - Total hours worked in a work week;
  - How the employee's pay is paid (i.e. per hour, per week, piecemeal, etcetera);
  - Regular hourly pay rate;
  - Total straight-time earnings;
  - Total overtime earnings per work week;
  - All additions to or deductions from employee's wages (i.e. withholdings, garnishments, payments for fringe benefits, etcetera);
  - Total wages paid each pay period; and
  - Dates of payment and the pay periods covered by each pay check.
- **Time Period for Maintaining Records**.
  - Three years for payroll records, collective bargaining agreements, sales and purchase records.
  - Two years for retention of wage computation records, including but not limited to time cards, piece work tickets, wage rate tables, work and time schedules and records of additions to and deductions from employee wages.

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. For 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.

D. The Rejection Letter. Well-written rejection letters can promote company goodwill. However, there are certain considerations to keep in mind to avoid potential legal issues, such as discrimination claims and/or failure to hire claims.

- There is no legal requirement to provide a rejection letter.
- Keep it short and simple, and be gracious and polite.
- Thank the applicant for applying for the position.
- Make sure the letter is factual.
- If providing a reason for the rejection, choose the wording carefully to avoid misinterpretation.
- Avoid discussing the qualifications and experience of other candidates, such as saying that employer decided to hire another candidate with more experience or better qualifications.
- Follow record retention requirements. [*SEE* RECORD RETENTION REQUIREMENTS, SECTION C.4 – THE JOB OFFER LETTER ABOVE]
- When rejecting employment based on a consumer report (i.e. criminal background check), ensure compliance with the FCRA. [*SEE* FCRA, SECTION C.2(a) – THE JOB OFFER LETTER ABOVE]

E. Checklist for a Legal Hire.

1. Practical Tips to Hiring.

a. **Design the Application**.

- Ensure applications do not improperly inquire about an applicant's race, color, sex, national origin, religion, age or any disability-related inquiries.
- Provide reasonable accommodations to those who need assistance in applying for positions.
- If a prospective candidate does not speak or read English well, in some circumstances, consider providing the application in different languages.

b. **Perform Background Checks**.

i. Criminal History.

- In April 2012, the EEOC issued new guidance in response to the Third Circuit Court of Appeals' decision in *El v. Southeastern Pennsylvania Transportation Authority*, 479 F.3d 232 (3d Cir. 2007), which found that an employer's criminal background policy was consistent with business necessity and did not violate Title VII. In *SEPTA*, the Court criticized the EEOC's guidelines and the thoroughness of its analysis and research on the use of criminal history information.
- EEOC recently filed two cases claiming employers violated Title VII for implementing and utilizing criminal background checks.
  - *EEOC v. BMW Manufacturing Co., LLC*, Case No. 7:13-cv-01583-HMH-JDA (D. S.C. June 11, 2013)
  - *EEOC v. DolGenCorp, LLC*, Case No. 1:2013-cv-04307 (N.D. Ill. June 11, 2013)
- EEOC Guidance on Conviction and Arrest Records provides best practice tips for employers:
  - Remove employment policies or practices that reject applicants from employment based on *any* criminal record.

- Train managers, hiring professionals and personnel decision makers about Title VII and its prohibitions.
- Develop narrowly tailored policies for screening job applicants and employees based on criminal history.
- When questioning applicants about prior criminal histories, limit it to criminal practices that are job related for the position. (i.e. theft/embezzlement for a bank teller position).
- Keep information about applicant and employee criminal screening confidential.

ii. GINA Compliance. Ensure not requesting genetic information of applicant in hiring decision or in post-employment medical examinations.

- **Coverage**. GINA applies to employers with 15 or more employees.
- **Protection**. GINA is designed to protect all individuals against discrimination in employment based on their genetic information.
- **Prohibits**.
  - GINA prohibits retaliation against employees who oppose discrimination protected by GINA or who participate in the investigation of alleged violations of GINA.
  - GINA also makes it unlawful for and prohibits an employer to request, require or purchase an employee's genetic information, except in limited circumstances. These circumstances include:
    - Compliance with family and medical leave laws;
    - Genetic monitoring of the effects of toxic substances in the workplace; and
    - DNA analysis for law enforcement purposes.
- **Case Law**.

- *EEOC v. Fabricut, Inc.*, Case No. 13-cv-248-CVE-PJC (N.D. Ohio May 7, 2013) (in a pending suit, the employer refused to hire an applicant because it regarded her as having carpal tunnel syndrome and rescinded its job offer and the EEOC claims it violated GINA when it inquired about her family medical history in its post-offer medical examination).
- *EEOC v. Founders Pavilion, Inc.*, Case No. 6:13-cv-06250 (W.D. N.Y. May 16, 2013) (employer violated GINA and other anti-discrimination statutes when it asked for genetic information in the post-hire medical examination).

iii. Off-Duty Conduct. If screening and considering an applicant's off-duty conduct in hiring, be sure to check applicable state off-duty conduct statutes. [*SEE* OFF-DUTY CONDUCT STATUTES, SECTION F.5(d) – USE OF SOCIAL MEDIA IN THE HIRING PROCESS BELOW]

iv. Negligent Hiring. Check employment references, the accuracy of submitted job applications and resumes, and investigate prospective employees' backgrounds to avoid tort claims for negligent hiring. Negligent hiring is where an employer knew or should have known of a prospective employee's propensity to be dangerous or liable for harm, which could have reasonably been foreseen at the time of hiring, including:

- Criminal background, if applicable.
- Driving records, if applicable.
- Credit history, if applicable.

v. State Laws. Some states, such as Florida, allow for a statutory presumption that an employer was not negligent in the hiring of an employee, where the employer conducted a background investigation of the prospective employee and the investigation did not reveal any

information that demonstrated an employee's unsuitability for work or for particular type of work. *See* Florida Statute §768.096.

vi. Compliance. When rejecting employment based on a consumer report, such as a criminal background report, ensure compliance with the FCRA. [*SEE* FCRA, SECTION C.2(a) – THE JOB OFFER LETTER ABOVE]

c. **Perform Reference Checks**. Call references and check accuracy of resume and application.

d. **Draft Offer Letter**. Review the offer letter for any potential legal issues and in light of the considerations discussed above.

e. **Provide Employee Handbook**.

- Provide the employee handbook at the time of hire.
- If the workforce does not speak or read English, consider providing a copy of the handbook to those employees in a different language they understand.
- For more details on employment handbooks, please refer to materials by another speaker in today's seminar. [*SEE* PROGRAM VII – EMPLOYEE HANDBOOKS AND POLICIES BY EVELYN P. SCHONBERG]

f. **Make Job Classification At Time of Hire**. Ensure employees are classified and paid properly in compliance with the FLSA (i.e. exempt, non-exempt from overtime).

g. **Comply with Record Retention Requirements**. Maintain records in accordance with record retention requirements. [*SEE* RECORD RETENTION REQUIREMENTS, SECTION C.4 – THE JOB OFFER LETTER ABOVE]

h. **Provide Notice of Need to Sign Non-Compete**.

- Can be enforceable in many states, but check applicable state law as to enforceability of non-competition/non-solicitation agreements. For example, in California, non-competes are void, except in very limited circumstances.

- Are used to protect legitimate business interests, such as customer relationships, confidential business information, business practices, marketing plans, and etcetera.
- Advise new hires whether they will be required to sign a non-compete and/or non-solicitation agreement as a condition of employment.
- Make sure it is in writing and is signed by all parties.
- Keep a copy of the signed non-compete agreement and/or non-solicitation agreement and provide a copy of the fully executed agreement to the employee.
- Ensure that non-compete and/or non-solicitation agreements are not overbroad and are reasonable in geographic and temporal scope.
- If employees do not speak, read or understand English well, have the non-competition/non-solicitation agreements available in different languages as an accommodation so employees can understand what they are signing.

i. **Have Employees Sign Confidential Proprietary Agreements**.

- Create and implement policies regarding confidential proprietary information and computer and/or data use.
- Include policies prohibiting employees from taking, copying or otherwise saving company information or data on personal computers, hard-drives, devices, e-mail systems, etcetera.
- Have employees sign an acknowledgement form regarding computer use and confidential information policies.

j. **Policy on Social Media**.

- Address ownership of social media accounts, the contents of the social media site as well as contacts at the time of hire.
- Explain who owns the social media as set forth below. [*SEE* WHO OWNS SOCIAL MEDIA, SECTION F.4 – USE OF SOCIAL MEDIA IN THE HIRING PROCESS BELOW]

- Do not ask for employee or applicant passwords or disclosure of social media contact in certain states. [*SEE* STATE LAWS THAT IMPACT THE USE OF SOCIAL MEDIA IN HIRING, SECTION F.5 – USE OF SOCIAL MEDIA IN THE HIRING PROCESS BELOW]
- Include social media policies in handbooks. For more details on employment handbooks, please refer to materials by another speaker in today's seminar. [*SEE* PROGRAM VII – EMPLOYEE HANDBOOKS AND POLICIES BY EVELYN P. SCHONBERG]

k. **Complete all Necessary Forms At Hire**.
- Tax forms;
- I-9 Employment Verification forms [*SEE* SECTION G – IMMIGRATION COMPLIANCE DOCUMENTS (I-9 AND E-VERIFY) BELOW];
- Insurance forms.

2. Common Employment Laws Impacting Hiring Decisions.

a. **Civil Rights Act of 1866, 42 U.S.C. §1981**. Prohibits discrimination based on race, color and/or ancestry and retaliation.

b. **Title VII**. Prohibits discrimination based on race, color, national origin, religion, gender, pregnancy and retaliation.

c. **ADEA**. Prohibits discrimination based on age over 40 years old and retaliation.

d. **ADA**. Prohibits discrimination based on disabilities, records of disability, and/or perceived disability and retaliation.

e. **EPA**. Prohibits gender discrimination in pay practices and retaliation.

f. **FCRA**. Governs use of consumer reports in hiring practices.

g. **FLSA**. Governs payment of minimum wage and overtime compensation.

h. **GINA**. Prohibits genetic information discrimination.

i. **Uniformed Services Employment and Reemployment Act, 38 U.S.C. §4301, *et. seq.* (USERRA)**. Prohibits discrimination in hiring of uniformed service members or veterans and prohibits retaliation.

j. **Immigration Reform and Control Act, 8 U.S.C. 1324a, *et. seq.* (IRCA)**. Prohibits discrimination based on citizenship or national origin.

k. **Title XI of the Bankruptcy Act, 11 U.S.C §525 (Title XI)**. Prohibits discrimination based on bankruptcy filings of debtors under the Bankruptcy Act.

l. **State Anti-Discrimination Laws**.

m. **State Drug-Testing Statutes**.

F. Use of Social Media in the Hiring Process.

1. Increasing Use. Nearly three out of four hiring managers and recruiters check candidates' social media profiles.[2] When using social media in the hiring process, keep in mind:

   a. The laws regulating it;

   b. Preservation and record retention requirements; and

   c. Privacy considerations.

2. 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.

      - Case Law: Social Media Postings Protected Speech.
        - *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).
      - Case Law: Social Media Postings Not Protected Speech.
        - *Bland v. Roberts*, 857 F. Supp. 2d 599 (E.D. Va. 2012) (liking a Facebook® page is not protected speech).

[2] 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/

- *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.); *see also Spanierman v. Hughes*, 576 F. Supp. 2d 292 (D. Conn. 2008) (finding protected speech but no causal connection).

- Case Law: 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.

- *O'Connor v. Ortega*, 480 U.S. 709 (1987) (where public employees can have reasonable expectations of privacy in the workplace).
  - An expectation of privacy may be limited by employer practices and procedures or by regulation. *Id.*
  - Must weigh an employee's expectations of privacy against the government's need to monitor, control and ensure the efficient operation of the workplace. *Id.*
- *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).

3. Federal Laws To be Aware of In the Use of Social Media.

   a. **The Stored Communications Act, 18 U.S.C. §2701, *et seq*. (SCA).** The 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 were 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).

      - Accessing 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.

- *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 key-logger software to access plaintiff's email 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).

- 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 were 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 (below), the SCA and the Railway Labor Act).
- No Search. Legal experts disagree on the propriety of searching social media sites at all.
  - Some feel that, if an employer desires to see the entire contents of an employee's Facebook® profile, they should ask the employee to accept a friend request from the employer, and inform the candidate they can remove the employer as a friend once they have completed the search. Depending on what state you are in, this practice may violate state law.

- Others feel that an employer should not view social media profiles because of the likelihood the employer will become aware of protected characteristics such as age, race, marital status, etc.
- The courts still have not provided sufficient guidance in this area.

b. **The Computer Fraud and Abuse Act, 18 U.S.C. §1030 (CFAA).** A number of cases have involved employers alleging violations of the CFAA. The CFAA prohibits the unauthorized access of a computer (or exceeding authorized access of a computer) and obtaining information. 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).

- *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).
- *Contrast Lee v. PMSI, Inc*., 2011 U.S. Dist. LEXIS 52828 (M.D. Fla. May 6, 2011) (dismissing party's CFAA counterclaim where former employee only accessed her personal websites, such as Facebook®, personal email, and news websites from employer's computer and did not improperly access employer information).

c. **The Electronic Communications Privacy Act, 18 U.S.C. §2510, *et seq*., a/k/a the Federal Wiretap Act (ECPA).** Title I of the 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. 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).

- No Interception. Courts will likely find that viewing Internet postings or web-pages, such as Facebook® and Twitter, does not constitute an interception under the ECPA:
  - *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).
  - *See also 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").

d. **FCRA Potential Violations** [*SEE* FCRA, SECTION C.2(a) – THE JOB OFFER LETTER ABOVE].

- Treat Same as Background Search. 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 background searches 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.[3]
  - 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.
- State Laws Restricting Use of Credit Reports. Check applicable state law when using credit reports. Eight states currently have legislation

[3] *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).

preventing an employer's use of credit reports.[4]

4. State Protection. Another source that may provide protection of unauthorized access or interception is state law. Many states have laws similar to the ECPA that prohibit the interception and/or unauthorized access to stored communications or communications in transit.
5. Who Owns Social Media.
   a. **Arising Issues**. Who owns the social media account, the contacts or the "friendships" especially when the employee who used, maintained or accessed the social media account leaves the employ of the employer?
   b. **Case Law**. Several courts have recently addressed whether an employer can assert an interest in social network accounts maintained by employees.
      - *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).
      - *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; case is currently pending and awaiting trial on whether a MySpace™ profile and friends constitutes a trade secret owned by the employer under Colorado law, among other things).
      - *Eagle v. Morgan*, 2011 U.S. Dist. LEXIS 147247 (E.D. Pa. Dec. 22,

[4] California (CAL. LAB. §1024.5; Connecticut (CONN. GEN. STAT. §31-51tt); Hawaii (HAW. REV. STAT. §378-2(8)); Illinois (820 ILL. COMP. STAT. 70/10); Maryland (MD. CODE ANN., LAB. & EMPL. §3-711); Oregon (OR. REV. STAT. §659A.885); Vermont (VT Act. No. 154, effective July 1, 2012); Washington (WASH. REV. CODE §19.182.005).

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).

- In 2008, at least one British court ruled on the ownership of content issue ordering a former recruiter to turn over his LinkedIn® contacts on his personal page to his former employer.

6. State Laws that Impact the Use of Social Media In Hiring.

   a. **State Laws Prohibiting Employers From Requesting Social Media Passwords.** State lawmakers began to introduce legislation to prevent employers from requesting social media password information from prospective employees and current employees in 2012. In 2012, 12 states had proposed legislation regarding employer access to social media. Presently, 12 states have legislation enacted prohibiting employers from requesting social media information from applicants or employees. Those states are: Arkansas, California, Colorado, Illinois, Maryland, Michigan, New Jersey, New Mexico, Oregon, Utah, Vermont and Washington.[5] In addition, as of June 3, 2013, there were at least 29 states with pending legislation.

   b. **States with Enacted Legislation[6]**.

      i. Oregon – H.B. 2654, codified in Chapter 204 (2013 Laws); Signed into law May 28, 2013; Effective January 1, 2014.

         - **Covered Employers**. The legislation does not define "employers", but the remedies section suggests that it also applies to public employers.
         - **Prohibitions**. This statute prohibits an employer from requiring, requesting or causing an employee or applicant to disclose or

[5] Delaware and New Jersey passed similar laws prohibiting educational institutions from requesting social media information from students.
[6] Listed in chronologically in order most recently enacted.

provide social media log-in information to a personal social media account. It is also an unlawful employment practice for an employer to compel an employee or applicant to add the employer to the employee's or applicant's list of contacts on their personal social media accounts. Further, the statute prohibits an employer from retaliating against an employee and/or refusing to hire an applicant who refuses to disclose or provide access to their social media accounts or to add the employer as a contact.

- **Exceptions**. The statute says that "an employer may require an employee to disclose any user name, password, or other means for accessing non-personal accounts that provide access to the employer's internal computers or information systems." No other exceptions are provided.
- **Remedies**. A person aggrieved under this statute has the right file a civil action in circuit court for equitable relief and damages (subject to limits on liability for public agencies), or both. The court shall award damages of $200 or actual damages, whichever is greater.

ii. Vermont – S.7, Act No.47; Signed into law May 24, 2013; Effective May 24, 2013. Initially, the bill was introduced and proposed legislation on prohibitions on employers accessing social media information from employees and/or applicants. However, the Senate revised the bill to create a Committee "to study the issue of prohibiting employers from requiring employees or applicants for employment to disclose a means of accessing the employee's or applicant's social media account." Essentially, the Committee will review legislation in other states and review the interplay with state law and proposed or existing federal law. The Committee is required to report its findings and propose legislation on or before January 15, 2014.

iii. Washington – RCW 49.44; Signed into law May 21, 2013; Effective July 28, 2013.

- **Covered Employers**. "Any person, firm, corporation, partnership, business trust, legal representative, or other business entity which engages in any business, industry, profession, or other activity in th[e] state and employs one or more employees, and includes the state, any state institution, state agency, political subdivision of the state, and any municipal corporation or quasi-municipal corporation."
- **Prohibitions**. This law prohibits an employer from requesting or requiring an employee or applicant to disclose log-in information for personal social networking accounts, or require an employee or applicant to provide the employer access to the content on the social media account. The statute also provides that an employer may not compel or coerce an employee or applicant to add a person, including the employer, to the list of contacts on the employee's or applicant's social media account. Further, the statute prohibits requesting or requiring an employee or applicant to alter the settings of their social media account. It also prohibits retaliation because an employee or an applicant refuses to disclose, access, add a person or alter the settings of their social media account pursuant to this statute.
- **Exceptions**. This law does not apply to an employer's request to share content of an employee's personal social network account when an employer is performing an investigation, whose purpose is to ensure compliance with applicable laws, regulatory requirements, or prohibitions against work-related employee misconduct; or to investigate an allegation of unauthorized transfer of an employer's proprietary information, confidential information

or financial data. Further, this law does not apply to the following: 1) a social network, intranet, or other platform that is intended primarily to facilitate work-related information exchange, collaboration, or communication by employees or other workers; 2) requesting or requiring an employee to disclose log-in information to access an account or service provided by virtue of the employment relationship or an electronic device or online account paid for or supplied by the employer; 3) to enforce existing personnel policies that do not conflict with this law; or 4) to comply with requirements of federal or state law.

- **Remedies**. A person aggrieved by a violation of this statute may bring a civil action in court to recover injunctive or other equitable relief, actual damages, a penalty in the amount of $500 and reasonable attorneys' fees and costs. This statute also allows a prevailing party to recover attorneys' fees and costs upon written findings that the action was frivolous and advanced without reasonable cause.

iv. Colorado – H.B. 13-10464; Signed into law May 11, 2013.

- **Covered Employers**. "A person engaged in a business, industry, profession, trade or other enterprise in the state or a unit of state or local government."
- **Prohibitions**. The law makes it unlawful for an employer to request or require an employee or applicant to disclose log-in information. It further prohibits an employer from discharging, disciplining or otherwise penalizing or threatening to discharge an employee or failing to hire an applicant because of his or her refusal to disclose any information specified in this statute.
- **Exceptions**. The law does not prohibit an employer from conducting an investigation to ensure compliance with applicable

securities or financial law or regulatory requirements; investigating an employee's communications based on information about improper use or authorized downloading of an employer's proprietary information or financial data.

- **Remedies**. A person aggrieved under this statute may bring a civil action in court within *one year* after the date of the alleged violation, in which the court may award injunctive relief, compensatory and consequential damages incurred and reasonable attorneys' fees and costs.

v. New Jersey – A2878; Passed March 21, 2013; Conditionally vetoed and revised based on Governor recommendations; Awaiting second reading in Senate.

- **Covered Employers**. Employer is defined broadly and means "an employer or employer's agent, representative or designee," but it has been revised to exclude the Department of Corrections, State Parole Board, county corrections departments or any State or local law enforcement agency.
- **Prohibitions**. The statute as revised based on the Governor's recommendations will prohibit an employer from requiring a current or prospective employee to provide or disclose any username or password or provide the employer access to a personal account or service. Further, it makes it unlawful for an employer to inquire whether an employee or prospective employee has a personal social networking account. An employer also may not require an individual to waive or limit any protection provided under this statute as a condition of employment. Any such limitation would violate public policy and is void and unenforceable. Lastly, the statute prohibits retaliation or discrimination against an individual because the individual a)

refused to provide or disclose username or passwords; b) report an alleged violation of the act to the Commissioner of Labor and Workforce Development; c) testify, assist or participate in an investigation, proceeding or action concerning a violation of this act; or d) otherwise oppose a violation of this act.

- **Exceptions**. The statute as revised provides that an employer is not prevented from conducting investigations for ensuring compliance with laws, rules and regulations or prohibitions against work-related employee misconduct based on information received about an employee's activity on a personal account; or investigating an employee for alleged transfers of proprietary information, confidential information or financial data. Further, the act does not prohibit an employer from viewing, accessing or using any information about a current or prospective employee that is available in the public domain. The employer is also free to implement policies regarding the use of employer-issued devices or accounts for business purposes. Lastly, an employer is not prohibited from complying with requirements of state or federal statues, rules or regulations.
- **Remedies**. An employer who violates this statute is subject to a civil penalty up to $1,000 for a first violation and up to $2,500 for each subsequent violation.

vi. Arkansas – H.B. 1901, to be codified at Arkansas Code 11-2-124; Signed into law April 22, 2013.

- **Covered Employers**. "Employer" means "a person or entity engaged in business, an industry, a profession, a trade, or other enterprise in the state or a unit of state or local government, including without limitation an agent, representative, or designee of the employer."

- **Prohibitions**. This law prohibits employers from requesting or requiring an employee or prospective employee to 1) disclose personal social media username and passwords; 2) add an employee, supervisor or administrator to the contacts associated with a personal social media account; or 3) change the privacy settings of the personal social media account. In addition, the statute makes it unlawful for an employer to take any adverse action or threaten an adverse action against an employee or fail to hire or refuse to hire a prospective employee because they exercise their rights under this statute.
- **Exceptions**. These prohibitions do not prevent an employer from complying with federal or state laws or regulations, or from requesting social media information if the employee's social media account is reasonably believed to be relevant to an investigation or related process in violation of federal or state law or employer policies.
- **Remedies**. This statute is silent as to potential remedies for violations of this statute.

vii. New Mexico – S.B. 371; Signed into law April 5, 2013; Effective July 1, 2013.

- **Covered Employers**. The statute does not define employer, but clearly states that this law does not apply to federal, state or local law enforcement agencies.
- **Prohibitions**. It is illegal for an employer to require or request a prospective employee to provide username and password information for the prospective employee's social media accounts. The statute does not appear to apply to current employees.
- **Exceptions**. It does not prevent an employer from: 1) having work place policies governing internet use, social networking site use

and e-mail use; and 2) monitoring use of the employer's electronic equipment or e-mail systems. Further, it expressly does not prohibit federal, state or local government agencies from conducting background checks as required by law.

- **Remedies**. The statute is silent as to potential remedies or causes of action for violations of this statute.

viii. Utah – H.B. 100, to be codified at UTAH CODE ANN. §§34-48-101–301. Title: Internet Employment Privacy Act; Signed into law March 26, 2013; Effective May 14, 2013.

- **Covered Employers**. "Employer" means a person, including the state or a political subdivision of the state, which has one or more workers or operators employed in the same business, or in or about the same establishment, under any contract of hire, express or implied, oral or written.
- **Prohibitions**. The Act prohibits employers from: 1) requesting an employee or an applicant for employment to disclose a username and password, or a password that allows access to the employee's or job applicant's personal Internet account; or 2) taking adverse action, failing to hire, or otherwise penalizing an employee or applicant for failure to disclose information described in Subsection 1. A "personal Internet account" means an online account that is used by an employee or applicant exclusively for personal communications unrelated to any business purpose of the employer and excludes an account created, maintained, used, or accessed by an employee or applicant for business-related communications or for a business purpose of the employer. "Adverse action" means to discharge, threaten, or otherwise discriminate against an employee in any manner that affects the employee's employment, including compensation, terms,

conditions, location, rights, immunities, promotions, or privileges.

- **Exceptions**. The Act does not prohibit an employer from: 1) requesting or requiring an employee to disclose a username or password required only to gain access to an electronic communications device supplied by or paid for in whole or in part by the employer, or an account or service provided by the employer, obtained by virtue of the employee's employment relationship with the employer, and used for the employer's business purposes; 2) disciplining or discharging an employee for transferring the employer's proprietary or confidential information or financial data to an employee's personal Internet account without the employer's authorization; 3) conducting an investigation or requiring an employee to cooperate in an investigation if there is specific information about activity on the employee's personal Internet account, for the purpose of ensuring compliance with applicable laws, regulatory requirements, or prohibitions against work-related employee misconduct, or the employer has specific information about an unauthorized transfer of the employer's proprietary information, confidential information, or financial data to an employee's personal Internet account; 4) restricting or prohibiting an employee's access to certain websites while using an electronic communications device supplied by or paid for in whole or in part by the employer or while using an employer's network or resources, in accordance with state and federal law; or 5) monitoring, reviewing, accessing, or blocking electronic data stored on an electronic communications device supplied by or paid for in whole or in part by the employer, or stored on an employer's network, in accordance with state and federal law. The Act also does not prohibit an employer from:

conducting an investigation or requiring an employee to cooperate in an investigation required by applicable law and regulations; prohibiting or restricting an employer from complying with a duty to screen employees or applicants before hiring or to monitor or retain employee communications that is established under federal law, by a self-regulatory organization or in the course of a law enforcement employment application or law enforcement officer conduct investigation performed by a law enforcement agency. The statute does not restrict an employer from viewing, accessing, or using information about an employee or applicant that can be obtained without accessing social media information that violates this statute or that is otherwise available in the public domain. Further, the Act makes it clear that it does not "create a duty for an employer to search or monitor [employees' or applicants'] personal internet accounts. In addition, "an employer is not liable…for failure to request or require that an employee or applicant grant access to, allow observation of, or disclose information that allows access to or observation of the employee's or applicant's personal Internet account."

- **Remedies**.

  (1) A person aggrieved by a violation of this chapter may bring a civil cause of action against an employer in a court of competent jurisdiction.

  (2) In an action brought under Subsection 1, if the court finds a violation of this chapter, the court shall award the aggrieved person not more than $500.

ix. California – Cal Lab Code §980: Signed into law on September 27, 2012; Effective January 1, 2013.

- **Covered Employers**. While the new statute does not explicitly

define “employer,” California is currently seeking to amend this law (A.B. 25) to apply to public employers, which indicates that the law does not presently apply to state or local government employers.

- **Prohibitions**. The law prohibits an employer from requesting or requiring an employee or applicant to: 1) disclose a username or password for the purpose of accessing personal social media; 2) access personal social media in the presence of the employer; and 3) divulge any personal social media except under certain circumstances. The law also prohibits an employer from discharging, threatening to discharge or otherwise discriminating against an employee or applicant for not complying with a request for social media information in violation of this law.
- **Exceptions**. The law permits an employer to request personal social media information relevant to an investigation of employee misconduct or violation of law, rule or regulation or for the purpose of accessing an employer-issued electronic device.
- **Remedies**. The statute is silent as to the potential remedies or penalties for violations of this law.

x. Illinois – 820 ILCS 55/10 §10(b)(1): Signed into law on August 1, 2012 and amended The Right to Privacy in the Workplace Act (RPW Act); Effective January 1, 2013.

- **Covered Employers**. The RPW Act does not define “employer” for purposes of the RPW Act. However, pending legislation (H.B. 1047) defines employer as “a person engaged in a business, industry, profession, trade, or other enterprise in this State, or any unit of State or local government.”
- **Prohibitions**. The law states that it is unlawful for an employer to request or require an employee or prospective employee to provide

any password or related account information to gain access to the employee's or prospective employee's account or profile on a social networking website or to demand access to the employee's or prospective employee's account or profile on a social networking website.

- **Exceptions**. An employer is not prohibited from: 1) promulgating workplace policies on use of employer's electronic equipment and social media; 2) monitoring usage of an employer's electronic equipment; or 3) requiring an employee to give passwords for social media accounts on the employer's devices.
- **Remedies**. The Illinois Legislature did not provide any specific remedies or penalties for violating this new law.
- **Amendments Pending**. Illinois currently has pending legislation (H.B. 1047) to clarify that an employer is prohibited from seeking this information from an employee or applicant's *personal* online account.
  - The amendments, if passed, will also provide additional exceptions to when an employer can request social media information, such as when the devices are supplied by or paid for in whole or in part by the employer or if the social media accounts are provided for by the employer or associated with the employee's employment by virtue of the employment relationship.
  - The amendments will also make it clear that it is an unlawful employment practice for an employer to discharge, discipline or otherwise penalize or threaten to discharge, discipline or otherwise an employee for their refusal to disclose information protected under this statute or to refuse to hire any prospective employee based on their refusal to provide information

protected under the statute.

- Under the amendments, an employer also cannot be held liable for any failure to request or require disclosure of an employee or prospective employee's personal social media accounts.
- Further, the amendments clarify the exceptions to provide that an employer is not prohibited from requesting the information as part of an investigation regarding: 1) compliance with laws, rules; and/or 2) regulations or prohibitions on employee misconduct; or 3) to protect the security and integrity of the employer's computers, devices networks of data if there is evidence that an employee has compromised the security and integrity of the employer's computers and devices; or 4) unauthorized transfer of an employer's proprietary information.
- Lastly, the amendments will provide definitions previously lacking from RPW Act.

xi. Michigan – Internet Privacy Protection Act, Public Act 478 of 2012 (IPPA), codified at MICH. COMP. LAWS §§37.272-.278; Signed into law December 27, 2012; Effective December 28, 2012.

- **Covered Employers**. This law applies to the employer, which is defined as "a person, including a unit of state or local government, engaged in a business, industry, profession, trade, or other enterprise in the state."
- **Prohibitions**. The IPPA makes it unlawful for an employer to "(i) request an employee or an applicant for employment to grant access to, allow observation of, or disclose information that allows access to or observation of the employee's or applicant's personal Internet account; and (ii) discharge, discipline, fail to hire, or otherwise penalize an employee or applicant for employment for failure to grant access to, allow observation of, or disclose

information that allows access to or observation of the employee's or applicant's personal Internet account."

- **Exceptions**. The IPPA does not prohibit an employer from: 1) requesting or requiring an employee to disclose access information to gain access to an electronic device paid for in whole or in part by the employer, an account or service provided by the employer; 2) disciplining or discharging an employee from transferring confidential proprietary information or financial data to an employee's personal Internet account without authorization; 3) conducting an investigation regarding: employee misconduct or violations of law, rule or regulation, transfers of confidential proprietary information; 4) monitoring electronic devices paid for by the employer; and 5) restricting an employee's access to certain websites using electronic devices paid for or provided by the employer.
- **Remedies**. If an employer violates the IPPA, the employer is guilty of a misdemeanor punishable by a fine of not more than $1,000. In addition, an employee can bring a civil action against the employer for damages not more than $1,000 plus reasonable attorneys' fees and costs.

xii. Maryland – Md. Labor & Employment Code §3-712: Signed into law on May 2, 2012; Effective October 1, 2012.

- **Covered Employers**. This law applies to the employer who is defined as "a person engaged in a business, an industry, a profession, a trade or other enterprise in the state; or a unit of State or local government."
- **Prohibitions**. An employer is prohibited from requesting or requiring disclosure of any username, password or other means for accessing personal social media accounts of employees or

applicants. Further, an employer cannot discharge, threaten to discharge, discipline or otherwise penalize an employee for not disclosing such information and prohibits an employer from refusing to hire an applicant for refusing to provide such protected information. The law also states that an employee may not download employer proprietary information without employer authorization to an employee's personal social media site or profile, web-based account or similar account.

- **Exceptions**. An employer may require disclosure for "accessing non-personal accounts or services that provide access to the employer's internal computer or information systems." Also, an employer is not prohibited from investigating compliance with applicable laws or regulatory requirements or employee conduct related to the improper download of proprietary information or financial data.
- **Remedies**. This law is silent as to potential remedies or penalties for violations of this statute.

c. **States with Pending Legislation**.

Arizona	Louisiana	Nebraska	Pennsylvania
California	Maine	Nevada	Rhode Island
Connecticut	Maryland	New Hampshire	Texas
Georgia	Massachusetts	New Jersey	West Virginia
Hawaii	Minnesota	New York	Wisconsin
Illinois	Mississippi	North Carolina	
Iowa	Missouri	North Dakota	
Kansas	Montana	Ohio	

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.

d. **Off-Duty Conduct Statutes**. Theoretically, existing "off-duty conduct" statutes, sometimes also referred to as "lawful products" or "lifestyle protection" statutes, could prohibit an employer from taking adverse action against an employee or job applicant based on the employee's/applicant's social media page reflecting the person engaging in some form of off-duty, off-premises lawful conduct. For example, an employer may be prohibited from making an employment-related decision based on seeing a picture of an over-21 employee or applicant consuming alcohol.[7] Besides elements of proof, there are two additional severe restrictions on the application of such statutes vis-à-vis social media and workplace. First, the application of a majority of these statutes is limited to tobacco use,[8] and second, all of these statutes exempt conduct having any connection with the employer's business concerns. An employer could therefore argue that publicizing drinking would be detrimental to the image of the business.[9] Five of these "off-duty" statutes (in California,

[7] *See, e.g.*, MINN. STAT. ANN. §181.938(2), which specifically includes alcohol as a lawful consumable product.

[8] *See* Marisa Anne Pagnattaro, *What Do You Do When You are Not at Work?: Limiting the Use of Off-Duty Conduct as the Basis for Adverse Employment Decisions*, 6 U. PA. J. LAB. & EMP. L. 625, 641 (2004); Jason Bosch, *None of Your Business (Interest): The Argument for Protecting All Employee Behavior With No Business Impact*, 76 S. CAL. L. REV. 639, 654-58 (2003) (describing the nature and benefits of "lifestyle protection statutes"). Seventeen states give protection for those who use tobacco: Connecticut (CONN. GEN. STAT. §24-34-402.5); Indiana (IND. CODE §22-5-4-1); Kentucky (KY. REV. STAT. ANN. §344.040); Louisiana (LA. REV. STAT. ANN. §23.966); Maine (ME. REV. STAT. ANN. Tit. 26, §597); Mississippi (MISS. CODE ANN. §71-7-33); New Hampshire (N.H. REV. STAT. ANN. §275:37-a); New Jersey (N.J. STAT. ANN. §34:6B-1); New Mexico (N.M. STAT. §50-11-3); Oklahoma (OKLA. STAT. tit. 40, §500); Oregon (OR. REV. STAT. §659A.315); Rhode Island (R.I. GEN. LAWS §23-20.10-14); South Carolina (S.C. CODE. ANN. §41-1-85); South Dakota (S.D. CODIFIED LAWS §41-1-85); Virginia (VA. CODE. ANN. §§2.2-2902, 15.2-1504); West Virginia (W. VA. CODE §21-3-19); and Wyoming (WYO. STAT. ANN. §27-9-105). Only eight states protect the use of lawful products without expressly limiting them to tobacco: Illinois (820 ILL. COMP. STAT. ANN. §55/5); Minnesota (MINN. STAT. §181.938); Missouri (MO. REV. STAT. §290.145); Montana (MONT. CODE ANN. §39-2-313); Nevada (NEV. REV. STAT. §613.333); North Carolina (N.C. GEN. STAT. §95-28.2(b)); Tennessee (TENN. CODE ANN. §50-1-304); Wisconsin (WIS. STAT. ANN. §111.31).

[9] *Cf. Miners v. Cargill Communc'ns, Inc.*, No. C8-97-837, 1997 WL 757157, at *3 (Minn. Ct. App. Dec. 9, 1997) (concluding that firing an employee after being involved in an accident while driving a company-owned van while intoxicated did not violate Minnesota's "lawful product" statute because the statute does not prohibit an employer from firing an employee for driving a company vehicle after consuming alcohol).

Colorado, Connecticut, New York and North Dakota) go beyond just lawful consumable products and protect off-duty conduct in general. However, these statutes have been interpreted by the courts infrequently and, despite their broad language, their actual applications reveal their limitations.

- California. In California, §96(k) of the California Labor Code authorizes the Labor Commissioner to take assignments of "[c]laims for loss of wages as the result of demotion, suspension, or discharge from employment for lawful conduct occurring during nonworking hours away from the employer's premises."[10] A plain reading of California's "lawful conduct" statute indicates there is no limitation to the type of lawful conduct protected. In *Barbee v. Household Automotive Finance Corp.*,[11] the California Court of Appeal rejected an employee's claim that his employer violated his (state) constitutional right of privacy[12] when the employer discharged him as a result of his intimate relationship with a co-worker.[13] The court concluded the employee had no reasonable expectation of privacy as to the relationship because he was on notice of the employer's policy discouraging such relationships and the employer was aware of the relationship.[14] The employee in *Barbee* claimed that his employer's conduct violated §96(k) because the intimate relationship with the co-worker took place during nonworking hours away from the employer's premises.[15] The court rejected this claim, holding that §96(k) "does not set forth an independent public policy that provides employees with any substantive rights, but rather, merely establishes a procedure by

[10] CAL. LAB. CODE §96(k).
[11] 6 Cal. Rptr. 3d 406 (Cal. Ct. App. 2003).
[12] *See* CAL. CONST. art. I, §1. The *Barbee* court stated that California's constitutional privacy provision applies to private, as well as public, actions. *See Barbee*, 6 Cal. Rptr. 3d at 410.
[13] *See Barbee*, 6 Cal. Rptr. 3d at 411.
[14] *See id*. at 411-12.
[15] *See id*. at 412.

which the Labor Commissioner may assert, on behalf of employees, recognized constitutional rights."[16] With no expectation of privacy, the employee had no invasion of privacy claim—and hence no claim—despite the action involving allegedly lawful conduct occurring during nonworking hours away from the employer's premises.

- Colorado. Colorado has enacted legislation which also prohibits an employer from terminating "the employment of any employee due to that employee's engaging in any lawful activity off the premises of the employer during nonworking hours."[17] However, Colorado's "lawful activity" restriction does not apply if the activity "[r]elates to a bona fide occupational requirement or is reasonably and rationally related to the employment activities and responsibilities of a particular employee."[18] Therefore, in *Marsh v. Delta Air Lines, Inc.*, the U.S. District Court ruled that an employer did not violate Colorado's statute when it dismissed an employee who had written a letter critical of management that was published in a newspaper.[19] The court held that the employee owed his employer a duty of loyalty, which the employee breached by trying to settle publicly a private dispute with management.[20]
- Connecticut. Connecticut's "off-duty" statute is limited to protecting employees who exercise state or federal first amendment rights.[21] At least as applied to free speech rights, courts have limited application of Connecticut's statute to speech relating to matters of public concern, and "internal employment policies are not a matter of public

[16] *Id*.
[17] COLO. REV. STAT. ANN. §24-34-402.5(1).
[18] *Id*. §24-34-402.5(1)(a).
[19] *See* 952 F. Supp. 1458, 1462 (D. Colo. 1997).
[20] *See id*. at 1463.
[21] CONN. GEN. STAT. ANN. §31-51q; *see also* Pagnattaro, *supra* note 8, at 669.

concern."[22]

- New York. The state of New York has adopted legislation that prohibits employers from discriminating against employees on the basis of their legal political activities, legal use of consumable products, and legal recreational activities—all off-site, outside of work hours without the use of the employer's equipment or other property.[23] The statute specifically excludes, however, any activity which "creates a material conflict of interest related to the employer's trade secrets, proprietary information or other proprietary or business interest."[24] To date, the majority of cases dealing with the "recreational activities" portion of the statute have defined recreational activities as not including romantic relationships or extramarital affairs,[25] although the Supreme Court, Appellate Division has ruled that an employee who was terminated as a result of a discussion during recreational activities (dinner at a restaurant) outside of the workplace in which her political affiliations became an issue, stated a cause of action for a violation of the state's statute.[26]
- North Dakota. North Dakota's statute prohibits discrimination by an employer, in part, based on an employee's "participation in lawful activity off the employer's premises during nonworking hours which is not in direct conflict with the essential business-related interests of the employer."[27] To date, only three cases have interpreted this particular language. In the first, the Supreme Court of North Dakota ruled it was

[22] *See, e.g., Daley v. Aetna Life & Cas. Co.*, 734 A.2d 112, 112-13 (Conn. 1999); *see also McClain v. Pfizer, Inc.*, 692 F. Supp. 2d 229, 242-43 (D. Conn. 2010).
[23] *See* N.Y. LAB. LAW §201-d(2)(a)-(c).
[24] *Id*. §201-d(3)(a).
[25] *See, e.g., State v. Wal-Mart Stores, Inc.*, 621 N.Y.S.2d 158 (N.Y. App. Div. 1995) (finding that legislative history of statute forbidding employer discrimination against employees excluded dating relationships from the definition of leisure activities); *McCavitt v. Swiss Reinsurance Am. Corp.*, 237 F.3d 166 (2d Cir. 2001) (finding same).
[26] *See Cavanaugh v. Doherty*, 675 N.Y.S.2d 143 (N.Y. App. Div. 1998).
[27] N.D. CENT. CODE §14-02.4-03.

a disputed issue of fact whether a chaplain who was discovered engaging in unseemly behavior in a Sears store bathroom was terminated for participating in lawful activity off the employer's premises during nonworking hours.[28] In *Jose v. Norwest Bank N.D., N.A.*, the North Dakota Supreme Court held that an employee's participation in an internal investigation of other employees' job performances was not a "lawful activity off the employer's premises during nonworking hours" entitled to protection under the statute.[29] And in 2012, the North Dakota Supreme Court held that an employee driving a company vehicle with a blood alcohol level above the limit imposed by the employer's policies conflicted with employer's essential business-related interests.[30]

As this brief review of lawful products/conduct statutes reveals, they have: 1) generated very few favorable decisions for employees or job applicants; and 2) have never been applied to a situation in which an employer or prospective employer has made an adverse employment decision based on social media content.

e. **Record Retention**. Maintain records in accordance with record retention requirements. [*SEE* RECORD RETENTION REQUIREMENTS, SECTION C.4 – THE JOB OFFER LETTER ABOVE]

7. Common Law Invasion of Privacy Considerations. Must also consider state common law protections when using social media in hiring.

- Generally, four types of common law invasion of privacy claims: 1) intrusion upon seclusion; 2) false light; 3) appropriation of likeness; and 4) public disclosure of private facts. The availability of these torts depends on varying state law and specific facts.
- Inquiries will be based on whether employees and/or applicants have an

[28] *See Hougum v. Valley Mem'l Homes*, 574 N.W.2d 812, 820 (N.D. 1998).
[29] 599 N.W.2d 293, 298 (N.D. 1999).
[30] *Clausnitzer v. Tesoro Ref. & Mktg. Co.*, 820 N.W.2d 665 (N.D. 2012).

expectation of privacy in their social media content and/or accounts.

a. **Case Law: No Claim for Invasion of Privacy**.

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

b. **Case Law: Invasion of Privacy Permitted**.

- *Ehling v. Monmouth-Ocean Hosp. Serv.*, 872 F. Supp.2d 369 (D.N.J. 2012) (invasion of privacy claim could proceed against employer who gained access to an employee's Facebook® posts through coercion, strong-arming and threatening another employee to give access to employer to view employee's Facebook® posts).
- *Coughlin v. Town of Arlington*, No. 10-10203-MLW, 2011 U.S. Dist. LEXIS 146285 (D. Mass. Dec. 19, 2011) (where employer gained access to an employee's personal e-mail accounts by monitoring the employee's work email, plaintiff sufficiently stated a claim for invasion of privacy).

G. Immigration Compliance Documents (I-9 and E-Verify™). The Immigration and Nationality Act, 8 U.S.C. §1101(1) (INA), governs employment eligibility for aliens, and includes:

1. Coverage.
   - INA applies to all employers; and
   - "Alien" is defined as any person who is not a citizen or national of the United States.
2. INA Requirements.
   - Employers are to hire only persons authorized to work in the United States, including aliens, so long as they are eligible to work.
   - Employers are obligated to verify identity and employment authorization by aliens. 8 C.F.R. §274a.2.

3. New Hire.

- Prior to or upon commencement of employment, an employee must complete the Employment Eligibility Verification form, also commonly referred to as Form I-9. 8 C.F.R. §274a.2(b)(1)(i)(A).
- Re-verification is required if employment authorization expires. The employer has an obligation to re-verify an employee's authorization to work by requiring the employee to provide documentation that shows continued eligibility to work in the United States or a new grant of work authorization. 8 C.F.R. §274a.2(b)(1)(vii).
- The re-verification must be completed before the expiration of the work authorization; otherwise the employee is no longer entitled to work in the United States.
- The re-verification should be reflected on the employee's Form I-9, and should include the date the employee's employment authorization expires.
- Three business days from commencement of work, an employer is to obtain the necessary documentation from the employee to verify authorization to work in the United States. 8 C.F.R. §274a.2(b)(1)(ii)(A)-(B).
    - Employer must physically examine non-expired documentation from the employee establishing the individual's identity and authorization to work in the United States.
    - An employee needs to provide documents to establish identity and work authorization, by providing either one document that establishes both; or by providing different documents that combined, establish both requirements.
    - Employer should not suggest which documents an employee is to provide for verification of employment to avoid discrimination claims.
- Examples of acceptable documents to establish both identity and employment authorization are:

- United States Passport; and
- Alien Registration Receipt Card or Permanent Resident Card. 8 C.F.R. §274a.2(b)(1)(v)(A).

- Examples of documentation sufficient to establish the individual's identity only for individuals over the age of 16[31]:
  - A driver's license or identification card issued by a state, with identifying information such as name, date of birth, sex, height, color of eyes and address;
  - School identification card with photograph;
  - Voter's registration card;
  - United States military card; or
  - Identification card issued by federal, state, or local government agencies. 8 C.F.R. §274a.2(b)(1)(v)(B).
- Examples of documentation sufficient to establish the individual's authorization to work in the United States only:
  - Social Security Account number;
  - Certification of Birth or Report of Birth issued by the Department of State;
  - An original or certified copy of a birth certificate issued by a state, county, local government bearing an official seal; or
  - Identification card for use of resident citizen in the United States. 8 C.F.R. §274a.2(b)(1)(v)(C).

4. Fraudulent Documents and Employer Obligations.

   a. **Review Documents for Authenticity**.

   - If the document looks genuine and relates to the person presenting the document, the employer must accept them. 8 C.F.R. §274a.2(b)(1)(ii)(A).

[31] Individuals under the age of 18 who cannot produce the listed documentation may produce different documentation to establish identity. *See* 8 C.F.R. §§274a.2(b)(1)(v)(B)(2)(i)-(iii).

- CAUTION: If employer does not accept a document that appears to be genuine, the employer may face claims for document abuse discrimination or other unfair immigration employment practices.
  - *See* 8 U.S.C. §1324a(b)(1)(A); *Collins Foods Int'l, Inc. v. INS*, 948 F.2d 549 (9th Cir. 1991) (an employer satisfies its verification obligations if the documents reasonably appear on their face to be genuine upon examination).
  - *Collins Foods Int'l, Inc.*, 948 F.2d at 553-554 (an employer is not required to compare the documents presented with the samples provided in the Immigration Services handbooks).
  - The U.S. Citizenship and Immigration Services *Handbook for Employers* gives guidance as to when verification documents may be questionable without a reasonable explanation for inconsistencies (available at Frequently Asked Questions, http://www.uscis.gov/files/form/m-274.pdf):
    - Where verification documents contain different last names;
    - Where verification documents contain different spellings of names; and
    - Where verification documents have compound last names.
  - Pursuant to 8 U.S.C. §1324a(a)(3), if after the hire, an employer learns or is put on notice that an employee's verification documents are questionable, the employer has a duty to investigate and resolve the concern, if possible.
    - *Zamora v. Elite Logistics, Inc.*, 478 F.3d 1160 (10th Cir. 2007) (noting that the Ninth Circuit has held that 8 U.S.C. §1324a(a)(2) adopts a "constructive knowledge standard," whereby "a deliberate failure to investigate suspicious circumstances imputes knowledge" to an employer, citing *New El Rey Sausage Co. v. INS*, 925 F.2d 1153, 1157-58 (9th Cir.

1991) (citations omitted), further the Court noted that "initial verification at the hiring stage is done through document inspection, but '[n]otice that these documents are incorrect places the employer in the position it would have been if the alien had failed to produce documents in the first place: it has failed to adequately ensure that the alien is authorized.'").

- If the document is questionable or does not appear to be genuine, the U.S. Citizenship and Immigration Services advises that an employer may not accept documents that do not appear to be genuine on their face as acceptable documentation. The employer is permitted to ask for other verification documentation if the individual presents questionable documents, or the employer can refuse to hire the individual without appropriate documents to verify authorization to work in the United States.

b. **Duty to Retain Documents**.

- For supporting documents establishing identity and authorization to work in the United States, the employer may, but is not required to, keep copies of the documents presented for completion of the Form I-9. 8 C.F.R. §274a.2(b)(3).
- If an employer chooses to retain copies of the documents, the employer is required to keep those copies with the completed Form I-9. 8 C.F.R. §274a.2(b)(3).

5. Record Retention. An employer is required to keep copies, electronic or in hard-copy, of all Form I-9's submitted on employees for a period of at least three years from the date of hire, or one year after the date the individual's employment is terminated, whichever is later. 8 C.F.R. §274a.2(b)(2)(i)(A).

a. **Inspection**. If requested by Department of Homeland Security (DHS), Office of Special Counsel (OSC) or the Department of Labor (DOL) to inspect the records, an employer must be given three days' advance notice

to make the records available in their original stored format (paper, electronic, etcetera). 8 C.F.R. §274a.2(b)(2)(ii).

b. **Type of Record**. Records can be completed and/or retained in paper form, microfiche or electronically, or any combination pursuant to DHS's standards on electronic retention, documentation, security and electronic signatures. *See* 8 C.F.R. §274.a.2(b)(2). However, if an employer uses E-Verify™ (discussed below), the employer must retain copies of the verification documents with photo identifications.

6. Common Errors.
   - Failing to get employee to sign the Form I-9.
   - Not completing within three days of employee commencing work.
   - Not listing date employment commenced.
   - Failing to re-verify upon expiration of an employee's employment authorization.
   - Not retaining records.
7. Good-Faith Defense. An employer is entitled to a rebuttable affirmative defense to alleged violations of the verification obligations if the employer can sufficiently show good-faith compliance with the employment verification requirements. 8 C.F.R. §274a.4. These apply to technical or procedural violations only. Additionally, employers have 10 days to correct non-compliance after receiving notice from the DHS.
8. Penalties for Non-Compliance. Under 8 C.F.R. §274a.10, the failure to complete a Form I-9 or knowingly hire persons unauthorized to work in the United States can include:
   a. **Monetary Penalties and Fines (from $110 to $1,110 per violation)**. These are determined based on five factors:
      - Size of employer's business;
      - Good faith of employer;
      - Severity of violation;

- Whether the individual is an unauthorized alien; and
- History of previous violations.

b. **Civil Penalties**. The civil penalties for knowingly hiring unauthorized aliens include:

- First Offense. Not less than $375 and not more than $3,200 for each unauthorized alien.
- Second Offense. Not less than $3,200 and not more than $6,500 for each unauthorized alien.
- Third Offense. Not less than $4,300 and not more than $16,000 for each unauthorized alien.

c. **Criminal Penalties**. Criminal penalties exist for engaging in a pattern or practice of knowingly hiring or continuing to employ unauthorized aliens.

d. **Injunctive Relief**.

9. Practical Tips for Compliance. Implement a compliance policy to include:

- Prohibition on the hiring of undocumented aliens NOT authorized to work in the United States.
- Designation of one department responsible for the completion and retention of Form I-9's, such as the Human Resources Department.
- Ensure documentation is readily accessible for inspection.
- Set up a system for reminding about deadlines for re-verification for those employees whose employment authorization will expire.
- Review Form I-9s for all new hires within a certain time frame to ensure compliance and no errors. Where errors or omissions are found, correct the Form I-9 and have the form initialed including a date that it was corrected.
- When using temp agencies, have strong indemnification agreements between the agency and employer for liability for employee eligibility.
- When relying on a third party to do employment verification, ensure that the third party assumes accountability and liability for completion of the

Form I-9. It is also important to ensure that the third party will have the documents accessible for inspection or audit.

10. Anti-Discrimination Provisions. There are different types of discrimination that are prohibited by the INA as well. The OSC enforces discrimination and retaliation complaints under the INA. INA discrimination and/or retaliation complaints must be filed within 180 days of the alleged discriminatory act:
    a. **Document Abuse**. Where an employer treats individuals differently because of national origin or citizenship status in the Form I-9 process. For example, requiring an employee to provide more documentation than is required, or requesting particular types of documents to establish identity and/or authorization to work.
    b. **Citizenship Status Discrimination**. This occurs when an employer treats employees differently based on their real or perceived citizenship or immigration status with respect to hiring, firing and recruitment.
    c. **National Origin Discrimination**. Discrimination based upon an employee's national origin in the hiring, firing and recruitment of employees. The INA national origin discrimination covers employers with more than three and less than 15 employees. Otherwise, national origin discrimination claims under Title VII where the employer has 15 or more employees are filed through the EEOC and must be filed within 180 days of the discriminatory act, unless the actions occurred in a deferral state extending the time frame to file to 300 days.
    d. **Retaliation**. INA prohibits retaliation against employees who have filed immigration related discrimination complaints, testified or participated in any immigration-related employment discrimination investigation, proceeding or hearing, or asserted rights under the INA anti-discrimination provisions.
11. E-Verify™.
    a. **What is E-Verify™**? E-Verify™ is an online system operated by the DHS

and the Social Security Administration (SSA). E-Verify™ is a web-based system that allows employers to file the Form I-9 or employment eligibility forms electronically to verify eligibility of an employee to work in the United States and check documentation online. It is used in conjunction with the Form I-9, not as a substitute for an employer's Form I-9 obligations.

b. **Who is Required to Use E-Verify™?**

- Federal agencies and private employers that apply to be or are federal contractors are required to use the E-Verify™ system. *See* Executive Order 12,989.
- Some states may require employers to use the E-Verify™ system, which was held to be permissible by the U.S. Supreme Court in *Chamber of Commerce of the U.S. v. Whiting*, 131 S. Ct. 1968 (2011).
  - Check applicable state laws where employer does business or has employees, not just where principal office or headquarters is located to determine whether E-Verify™ is mandatory and what employers are required to comply.
  - For example, Utah requires all employers with 15 or more employees to use E-Verify™, while Georgia only requires public agencies, contractors and subcontractors with 500 or more employees to use E-Verify™.
  - States may also have different fines/penalties associated with the failure to comply with E-Verify™ mandates.

c. **What is the Purpose of E-Verify™?** In theory, using E-Verify™ should insulate employers from civil and criminal liability for issues with employment of undocumented workers. However, just because an employer uses E-Verify™ does not protect an employer from liability for technical or procedural violations involving the completion of the Form I-9.

d. **Memorandum of Understanding (MOU)**. E-Verify™ participants are required to execute an MOU with the DHS and SSA. After signing the MOU, employers must use E-Verify™ for all new hires, creating two obligations:

- Completing Form I-9; and
- Completing the E-Verify™ inquiry.

e. **Border Security, Economic Opportunity, and Immigration Modernization Act (S. 744)**. Introduced on April 16, 2013, it is still before the Senate for review. If passed, this bill would make E-Verify™ mandatory for all employers, not just federal employers. The requirement of E-Verify™ would be subject to a phase-in over a five-year period.