UPDATE ON ETHICAL ISSUES AND SOCIAL MEDIA

by

Cynthia N. Sass, Esquire

American Bar Association
Section of Labor & Employment Law
Ethics and Professional Responsibility Committee
March 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

UPDATE ON ETHICAL ISSUES AND SOCIAL MEDIA[1]

Moderator: Myra McKenzie, Esquire
Speakers: John F. Hernandez, Esquire
Cynthia N. Sass, Esquire
Elizabeth Theran, Esquire

American Bar Association
Section of Labor and Employment Law
Ethics & Professional Responsibility Committee Midwinter Meeting

---

A. STATE LAWS PROHIBITING EMPLOYERS FROM REQUESTING SOCIAL MEDIA INFORMATION AND PASSWORDS

State law makers began to introduce legislation to prevent employers from requesting social media password information from employers in 2012. In 2012, 12 states had proposed legislation regarding employer access to social media. Presently, only four states have legislation enacted prohibiting employers from requesting social media information from applicants or employees. Those states are: California, Illinois, Maryland, and Michigan.[2] In addition, as of February 13, 2013, there were at least 28 states with pending legislation.

1. States with Enacted Legislation

a. 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 to apply to public employers, which indicates that presently the law does not apply to state or local government employers.
- **Prohibitions:** The law prohibits an employer from requesting or requiring an employee 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; 3) divulge any personal social media except under certain circumstances. The law also prohibits an employer from discharging, threatening

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

[2] Delaware and New Jersey passed similar laws prohibiting educational institutions from requesting social media information from students.

to discharge or otherwise discriminate against an employee for not complying with a request for social media information in violation of this law.

- **Exceptions:** However, 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.

b. 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.
- **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 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.

c. Michigan – Internet Privacy Protection Act, Public Act 478 of 2012 ("IPPA"). Signed into law December 27, 2012, effective December 28, 2012.

- **Covered Employers:** This law applies to employers, 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 1) "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; 2) 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.

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

- **Covered Employers:** This law applies to employers who are 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 improper download of proprietary information or financial data.
- **Remedies:** This law is silent as to potential remedies or penalties for violations of this statute.

2. **States with Pending Legislation**

Arizona	Kansas	Montana	Oregon
Colorado	Maine	Nebraska	Rhode Island
Connecticut	Maryland	New Hampshire	Texas
Georgia	Massachusetts	New Jersey	Utah
Hawaii	Minnesota	New Mexico	Vermont
Illinois	Mississippi	New York	Washington
Iowa	Missouri	North Dakota	

See **Appendix A** for the comprehensive list of the states with proposed legislation and cites to the actual proposed bills. 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.

B. COMPUTER LAWS THAT IMPACT SOCIAL MEDIA

1. **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 where appropriate (for willful or intentional violations), a reasonable attorney's fee and other litigation costs reasonably incurred. The SCA also states that in no case shall a person entitled to recover receive less than the sum of $1,000. 18 U.S.C. §2707. In addition, there are possible criminal penalties including a fine and imprisonment for up to 10 years. 18 U.S.C. §2701(b).

   a. 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).

      - *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).

      - *Pietrylo v. Hillstone Restaurant Group*, 2008 WL 6085437 (D.N.J. 2008). In *Pietrylo*, 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.

b. 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, the SCA and the Railway Labor Act.

c. 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. 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.

Employers should be aware of and conform to the requirements of background screening under the Fair Credit Reporting Act.

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

- *Eagle v. Morgan*, 2012 U.S. Dist. LEXIS 143614 (E.D. Pa. Oct. 4, 2012). In *Eagle*, the plaintiff was a former CEO of EdComm, a banking education company. When employed the plaintiff maintained a LinkedIn® account to promote the defendant's services, foster her reputation, reconnect with family and friends and colleagues and build relationships. Another employee assisted the plaintiff to maintain the account.

After the plaintiff was terminated, the employer used the plaintiff's LinkedIn® password to access her account and changed the password. Subsequently, the employer changed the profile information to announce the new CEO name and photo and removed the plaintiff as the CEO. However, the profile still had the previous CEO's experience and accomplishments on the profile. The plaintiff filed suit against EdComm under the CFAA, among other things, due to the employer's unauthorized access to her social media account. The court granted summary judgment for the defendant finding that the plaintiff could not prove a cognizable loss as a result of the access, which required a grant of summary judgment as to the CFAA claim.

3. **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, and it most often arises in the labor context where employers monitor and intercept communications between employees. However, under the ECPA, consent to the interception by one party to the communication is a defense to a violation.

   The ECPA provides for separate causes of action, both by private individuals and by the government. In a private cause of action under the ECPA, a plaintiff may recover preliminary and other equitable or declaratory relief as may be appropriate, declaratory damages, punitive damages where appropriate, reasonable attorney's fees and other litigation costs reasonably incurred. 18 U.S.C. §2520. Notably, the ECPA provides that the plaintiff will receive at a minimum $10,000, regardless of a showing of any actual damages. In addition, if the communication involves certain radio or private satellite video communications, the violator may be subject to suit by the federal government. 18 U.S.C. §2511(5). Finally, the ECPA provides for criminal penalties including a fine and imprisonment for up to five years. 18 U.S.C. §2511(4).

   a. <u>No Interception</u>. 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). In *Konop*, 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").

b. 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.

4. **Potential Violation of the Fair Credit Reporting Act**, 15 U.S.C. § 1681 *et seq.* **("FCRA")**.

a. Notification. The FCRA requires that employers notify applicants if consumer reports will be used in an employment decision. 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:

- a clear and conspicuous disclosure has been made in writing to the consumer at any time before the report is procured or caused to be procured, in a document that consists solely of the disclosure, that a consumer report may be obtained for employment purposes; and

- the consumer has authorized in writing (which authorization may be made on the document referred to in clause (i)) the procurement of the report by that person.

b. Consumer Report. A "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.**

c. Purpose. "Employment purposes" means a report used for the purpose of evaluating a consumer for employment, promotion, reassignment or retention as an employee.

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

e. 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, and give the candidate the opportunity to dispute negative information.

f. Penalties for Noncompliance. Noncompliance with the FCRA can result in civil penalties including a $1,000 fine, punitive damages and the award of attorney's fees and costs.

- 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.

C. EEOC RECORD RETENTION POLICIES AND THE IMPACT ON SOCIAL MEDIA

1. **Title VII, the ADA, and GINA:**[3] These Acts require the EEOC to establish regulations pursuant to which employers, labor organizations, joint labor-management committees, and employment agencies subject to these Acts shall make and preserve certain records and shall furnish specified information to aid in the administration and enforcement of the Acts. Those requirements are set out in 29 C.F.R. part 1602.

2. **Recordkeeping Provisions**: For our purposes here, we are concerned with the provisions on recordkeeping: Subpart C: Recordkeeping by Employers; Subpart G: Recordkeeping by Labor Organizations; and Subpart I: State & Local Governments Recordkeeping. There are also separate recordkeeping provisions for apprenticeship programs (Subpart E) and institutions of higher education (Subpart O). The point to keep in mind is that the advent of social media does not change any of these obligations. The fact that recruitment may now be online, or that job applications may come through Facebook® or craigslist, does not alter the employer's responsibility to preserve electronic data just as it would hard copies.

   a. Subpart C: Recordkeeping by Employers. §1602.12 explains that:

      > The Commission has not adopted any requirement, generally applicable to employers, that records be made or kept. It reserves the right to impose recordkeeping requirements upon individual employers or groups of employers subject to its jurisdiction whenever, in its judgment, such records (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.

   However, there are specific rules regarding preservation that apply when employers do keep such records, set out in 29 C.F.R. §1602.14.

   - Any personnel or employment record made or kept by an employer (including but not necessarily limited to requests for reasonable accommodation, application

[3] Title VII of the Civil Rights Act of 1964, 42 U.S.C. §2000e, et. seq. ("Title VII"), Americans with Disabilities Act of 1990, 42 U.S.C. § 12101, et seq. ("ADA"); and Genetic Information Nondiscrimination Act of 2008 ("GINA").

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) shall be preserved by the employer for a period of one year from the date of the making of the record or the personnel action involved, whichever occurs later.

- 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.

- Where a charge of discrimination has been filed, or an action brought by the Commission or the Attorney General, against an employer under Title VII, the ADA, or GINA, the respondent employer shall preserve all personnel records relevant to the charge or action until final disposition of the charge or the action.

b. Subpart G: Recordkeeping by Labor Organizations. Unlike the provision for private employers, §1602.27 specifies that all local, independent, or unaffiliated unions with 100 or more members (or their agents) are required to keep certain records with respect to the data underlying:

> [t]hose portions of Report EEO-3 calling for information about union policies and practices and for the compilation of statistics on the race, color, national origin, and sex of members, persons referred, and apprentices.

29 C.F.R. §1602.28 sets out the rules for preservation of these records:

- All records made by a labor organization or its agent solely for the purpose of completing Report EEO-3 shall be preserved for a period of one year from the due date of the report for which they were compiled.

- Any labor organization identified as a "referral union" in the instructions accompanying Report EEO-3, or agent thereto, shall preserve other membership or referral records (including applications for same) made or kept by it for a period of one year from the date of the making of the record.

- Where a charge of discrimination has been filed, or an action brought by the EEOC or the Attorney General, against a labor organization under Title VII, the ADA, or GINA, the respondent labor organization shall preserve all records relevant to the charge or action until final disposition of the charge or the action.

- Nothing in this section relieves a labor organization covered by Title VII of any obligation to comply with the recordkeeping requirements of Subpart E, pertaining to apprenticeship programs.

c. Subpart I: State & Local Governments Recordkeeping. State and local governments also have specific recordkeeping requirements. §1602.30 provides that, on an annual basis from September 30, 1974, onward, every political jurisdiction with 15 or more employees is required to make or keep records and the information therefrom which are or would be necessary for the completion of report EEO-4, regardless of whether the jurisdiction is actually required to file the EEO-4. The reports and/or the underlying information are required to be retained for a period of three years at the central office of the political jurisdiction and to be made available if requested by an officer, agent, or employee of the EEOC under section 710 of Title VII, as amended.

29 C.F.R. §1602.31 sets out the rules for preservation of these records:

- Any personnel or employment record made or kept by a political jurisdiction (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, layoff, or termination, rates of pay or other terms of compensation, and selection for training or apprenticeship) shall be preserved by the political jurisdiction for a period of two years from the date of the making of the record or the personnel action involved, whichever occurs later.

- In the case of involuntary termination of an employee, the personnel records of the individual terminated shall be kept for a period of two years from the date of termination.

- Where a charge of discrimination has been filed, or an action brought by the Attorney General against a political jurisdiction under Title VII, the ADA, or GINA, the respondent political jurisdiction shall preserve all personnel records relevant to the charge or action until final disposition of the charge or the action.

3. **GINA-Specific Regulations**: There are also GINA-specific regulations governing both acquisition of genetic information covered under the statute and confidentiality requirements that apply to that information, which are addressed in 29 C.F.R. §§1635.8 and 1635.9.

a. Acquisition of genetic information. 29 C.F.R. §1635.8 addresses the ways in which covered entities can and cannot acquire genetic information about individuals.

- §1635.8(a) sets out the general prohibition:

> A covered entity may not request, require, or purchase genetic information of an individual or family member of the individual, except as specifically provided in paragraph (b) of this section. 'Request' includes conducting an Internet search on an individual in a way that is likely to result in a covered entity obtaining genetic information; actively listening to third-party conversations or searching an individual's personal effects for the purpose of obtaining

genetic information; and making requests for information about an individual's current health status in a way that is likely to result in a covered entity obtaining genetic information.

- §1635.8(b) is a long, detailed section setting out six exceptions to §1635.8(a). In brief, the six exceptions are:

  (1) Where a covered entity inadvertently requests or requires genetic information of the individual or family member of the individual.

  (2) Where a covered entity offers health or genetic services, including such services offered as part of a voluntary wellness program.

  (3) Where the covered entity requests family medical history to comply with the certification provisions of the Family and Medical Leave Act of 1993, 29 U.S.C. §§2601, *et seq*. ("FMLA"), or State or local family and medical leave laws, or pursuant to a policy (even in the absence of requirements of Federal, State, or local leave laws) that permits the use of leave to care for a sick family member and that requires all employees to provide information about the health condition of the family member to substantiate the need for leave.

  (4) Where the covered entity acquires genetic information from documents that are commercially and publicly available for review or purchase, including newspapers, magazines, periodicals, or books, or through electronic media, such as information communicated through television, movies, or the Internet, EXCEPT that this exception does not apply to various sources with limited access or if the covered entity intended to obtain genetic information.

  (5) Where the covered entity acquires genetic information for use in the genetic monitoring of the biological effects of toxic substances in the workplace. In order for this exception to apply, the covered entity must provide written notice of the monitoring to the individual and the individual must be informed of the individual monitoring results.

  (6) Where an employer conducts DNA analysis for law enforcement purposes as a forensic laboratory or for purposes of human remains identification and requests or requires genetic information of its employees, apprentices, or trainees, but only to the extent that the genetic information is used for analysis of DNA identification markers for quality control to detect sample contamination and is maintained and disclosed in a manner consistent with such use.

- §1635.8(c) sets out two further exceptions to the general prohibition in §1635.8(a).

(1) A covered entity does not violate this section when it requests, requires, or purchases information about a manifested disease, disorder, or pathological condition of an employee, member, or apprenticeship program participant whose family member is an employee for the same employer, a member of the same labor organization, or a participant in the same apprenticeship program. For example, an employer will not violate this section by asking someone whose sister also works for the employer to take a post-offer medical examination that does not include requests for genetic information.

(2) A covered entity does not violate this section when it requests, requires, or purchases genetic information or information about the manifestation of a disease, disorder, or pathological condition of an individual's family member who is receiving health or genetic services on a voluntary basis. For example, an employer does not unlawfully acquire genetic information about an employee when it asks the employee's family member who is receiving health services from the employer if her diabetes is under control.

- §1635.8(d) addresses medical examinations related to employment:

> The prohibition on acquisition of genetic information, including family medical history, applies to medical examinations related to employment. A covered entity must tell health care providers not to collect genetic information, including family medical history, as part of a medical examination intended to determine the ability to perform a job, and must take additional reasonable measures within its control if it learns that genetic information is being requested or required. Such reasonable measures may depend on the facts and circumstances under which a request for genetic information was made, and may include no longer using the services of a health care professional who continues to request or require genetic information during medical examinations after being informed not to do so.

- §1635.8(e) provides that a covered entity may not use genetic information obtained pursuant to subparagraphs (b) or (c) of this section to discriminate against individuals, and must keep such information confidential as required by §1635.9.

b. Confidentiality. 29 C.F.R. §1635.9 addresses the confidentiality requirements as to genetic information once it has already been acquired by the covered entity.

- §1635.9(a) addresses confidential treatment of genetic information.

(1) A covered entity that possesses genetic information in writing about an employee or member must maintain such information on forms and in medical files (including where the information exists in electronic forms and files) that

are separate from personnel files and treat such information as a confidential medical record.

(2) A covered entity may maintain genetic information about an employee or member in the same file in which it maintains confidential medical information subject to section 102(d)(3)(B) of the ADA.

(3) Genetic information that a covered entity receives orally need not be reduced to writing, but may not be disclosed, except as permitted by this part.

(4) Genetic information that a covered entity acquires through sources that are commercially and publicly available, as provided by, and subject to the limitations in, §1635.8(b)(4) of this part, is not considered confidential genetic information, but may not be used to discriminate against an individual.

(5) Genetic information placed in personnel files prior to November 21, 2009, need not be removed and a covered entity will not be liable under this part for the mere existence of the information in the file. However, the prohibitions on use and disclosure of genetic information apply to all genetic information that meets the statutory definition, including this earlier information.

- §1635.9(b) addresses exceptions to the limitations on disclosure. It provides that a covered entity that possesses any genetic information, regardless of how the entity obtained the information (except for genetic information acquired through commercially and publicly available sources), may not disclose it except:

(1) To the employee or member (or family member if the family member is receiving the genetic services) about whom the information pertains upon receipt of the employee's or member's written request;

(2) To an occupational or other health researcher if the research is conducted in compliance with the regulations and protections provided for under 45 C.F.R. part 46;

(3) In response to an order of a court, except that the covered entity may disclose only the genetic information expressly authorized by such order; and the individual must be informed of the court order and the genetic information disclosed;

(4) To government officials investigating compliance with this title if the information is relevant to the investigation;

(5) To the extent that such disclosure is made in support of an employee's compliance with the certification provisions of section 103 of the FMLA or such requirements under State family and medical leave laws; or

(6) To a Federal, State, or local public health agency only with regard to information about the manifestation of a disease or disorder that concerns a contagious disease that presents an imminent hazard of death or life-threatening illness, provided that the individual whose family member is the subject of the disclosure is notified of such disclosure.

- §1635.9(c) addresses the relationship between GINA and HIPAA's[4] privacy regulations and provides that:

> Pursuant to § 1635.11(d) of this part, nothing in this section shall be construed as applying to the use or disclosure of genetic information that is protected health information subject to the regulations issued pursuant to section 264(c) of the Health Insurance Portability and Accountability Act of 1996.

D. USE OF CLEANERS TO PURGE INTERNET OR ON-LINE HISTORY

1. **What is a cleaner**? A cleaner is a software or service that may be used to clean up or erase a computer's Internet history, temporary internet files, computer cache and other files on a computer that have been viewed or downloaded from the Internet. As individuals use the Internet or other online sources, the computer creates temporary files to store information such as Internet browsing history and file download history. Cleaners are often used to make a computer more efficient by eliminating the sometimes unnecessary back up of temporary files. Others may use cleaners to erase the history or the footprint of their travels on the computer and Internet so others do not see what websites they have visited, what files have been downloaded, or what other types of files viewed on the computer, etcetera.

   a. Software: There is software that performs such cleaning. One of the most popular cleaners is "CCleaner" (http://www.piriform.com/ccleaner), but there are others available, such as Evidence Eliminator. Such software may be used by many companies IT's departments to maintain the security of computer networks, as well as clean up unnecessary files. However, there may be documents or files in the temporary files that could be responsive to discovery requests or show evidence of Internet history that may be relevant in litigation that could be purged or deleted through the use of these cleaners.

   b. Services that assist people to "clean" inappropriate content on different social media platforms:

      - **SocioClean**. A free service that allows users to purge any bad or inappropriate material from different social media sites to allow them to keep their social reputation clean. Socioclean works by scanning the user's social media profiles, including pictures, postings, messages and other items on public display. After the scanning process, SocioClean analyzes the public content and grades the content

[4] Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

for potential inappropriate material. SocioClean then provides the analysis to the user, who then has the discretion to go back and delete the negative information from their profiles. *See* http://socioclean.com.

- **Reppler**. A social media monitoring service that includes identification of potential issues and risks about content on social media profiles, which could result in users identifying the negative information and deleting it from the profile. *See* www.reppler.com.

- There are also a number of websites that provide services for businesses and individuals to clean up their online reputation, not by necessarily removing their on-line history, but by tactics to boost the positive results and bury the negative results when someone searches them on the Internet, such as Google™, Firefox®, Safari, etcetera. For an example of this type of service, refer to www.reputation.com.

These are just a few examples of the types of cleaners available to the average person, as well as companies, to purge computer temporary files, on-line histories and/or to help hide negative information available on the Internet.

2. **Ethical Concerns Involving the Use of Cleaners**. Although negative information on a client's Facebook® page may be detrimental to a client's case, a lawyer should think twice before advising clients (or directing their staff to advise clients) to "clean up" their social media profiles or to delete social media profiles. Such advice will result in the spoliation of evidence, which in turn could carry significant sanctions against the attorney and even the client and potential discipline of the attorney by the bar.

- *Lester v. Allied Concrete Co.*, 83 Va. Cir. 308, 2011 Va. Cir. LEXIS 245 (Sept. 2011); 83 Va. Cir. 308, 2011 Va. Cir. LEXIS 132 (Oct. 2011). Iin *Lester*, the court sanctioned an attorney and his client to the tune of $720,000 ($540,000 attributable to the attorney, $180,000 attributable to the client) in part for the attorney instructing the client to clean up his Facebook® page, which resulted in the client ultimately spoliating evidence by deleting numerous photos from his Facebook® page. In light of the attorney's actions in this case, the court referred a complaint to the Virginia State Bar.

3. **Practical Tips for Using Cleaners:**

a. Corporations should update their record retention policies and procedures to address cleaners, how often they are used to delete data and the protocols for potentially suspending the use of cleaners once litigation is anticipated.

b. Companies should regularly update company employee handbooks or electronic communications policies to advise employees that they are prohibited from downloading or using cleaners for business computers, devices and/or servers and put in place security protocols that prevent employees from downloading such programs to the company servers or individual work stations.

c. From the beginning of representation, when discussing an individual's duty to preserve evidence, lawyers should ask clients about the client's use of cleaners, whether there are any installed or currently used by the client. If the client uses cleaners, immediately instruct the individual to stop using the cleaners and document this in writing.

d. In addition, if the individual uses a cleaner on their personal computers, find out the frequency of using the cleaners, what types of files the individual uses the cleaner to delete. If you can show that the individual has a routine habit of performing "cleaning" on their computer, it may be easier to fight a potential spoliation of evidence claim later.

e. Lawyers should frequently train and instruct staff on social media and the practices that are and are not allowable under the rules to ensure that non-lawyers under the supervision of the lawyer do not engage in conduct that puts the lawyer at risk for sanctions and ethics violations.

E. NEW TECHNOLOGICAL ADVANCES AND IMPLICATIONS FOR LAWYERS

1. **"Temporary" Record**. The permanent nature and long-lasting effects of social media posts and other negative information available on the public domain prompted creators to develop new technologies that promise to allow the exchange of messages, pictures and videos without the permanent record. These technologies allow end users to use the application to send a text message, photo or video that self-destructs within a certain time frame after the recipient has viewed it. Examples of these types of applications are: Snapchat, Poke, Vidburn and Wickr. Presently, it appears that these applications are only available for Iphone and Android users.

2. **No Cases Yet**. Currently, there are no cases that discuss these new technologies, but as these technologies become more popular, it is likely that lawyers will start to face numerous issues involving such technological advances.

3. **Ethical Concerns and Spoliation**. These are two potential areas of issues that practitioners may face as these technologies become the norm. As we all know, the sanctions for spoliation of evidence could be significant and can adversely affect a case. Further, there are unanswered questions as to the ethics for lawyers and these new technologies.

   a. <u>To Use or Not to Use</u>. As these technologies emerge, one question that will need to be answered is whether it is ethically proper for a lawyer to instruct a client to use

such technologies. Based on the numerous ethics opinions on social media, it would appear that any bar association faced with this question will likely find that it is improper to advise clients to use applications that potentially destroy and keep no record of potentially relevant evidence.

b. Screen Shots? Lawyers may also have a duty to inform their clients to attempt to preserve and/or take screen shots of messages potentially relevant to action if the parties are involved in or anticipate litigation where the lawyer is aware that the client is using or has used these applications.

c. Knowledge a Must. Consistent with a lawyer's duty to be competent and aware of technological changes, lawyers should educate themselves about the varying types of technologies. Once the lawyer is aware of these technologies, the lawyer can inquire of clients about use of these technologies and evaluate the potential issues for a spoliation claim.

d. Update Policies. Such technologies may also necessitate corporations to update company handbooks and employment policies and procedures on the use of these types of technologies in the workplace without infringing upon employee rights to engage in concerted protected activities under the National Labor Relations Act.

4. **Preservation Possible**. However, these technologies may not prove as "temporary" as advertised.. For example, if users of these apps educate themselves, recipients of self-destructing messages may be able to use a screenshot function in order to preserve the messages for future use in litigation, etcetera. Moreover, in reality, these applications use some sort of server or on-line data backup that transmits the contents to the recipients. In other words, there should be a record of the messages somewhere. Thus, such messages may prove to be discoverable through use of subpoenas to the third-party service providers seeking discovery of messages from particular users. It is too early to tell how this will play out, but it is something to keep in mindful.

F. WHO ACTUALLY OWNS THE SOCIAL MEDIA PROFILE?

1. **Ownership**. Social media sites are commonly being used by employers and employees alike to help develop the employer's business or drum up business. One recent issue developing with respect to social media sites is who owns the 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. The line is often blurred on who owns the account and whether the information, friendships or connections are trade secrets or company proprietary property. The courts are only beginning to address these issues and the law on this area is in its infancy.

2. **Case Law**. Three courts have addressed whether an employer can assert an interest in social networking profiles maintained by employees or in an employee's name.

- *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) was the first to attack ownership of social media profiles. In *PhoneDog*, the employer brought suit against a former employee for the employee's use of a Twitter account that the employer claimed to own. PhoneDog is an interactive mobile news and reviews web source that uses multiple social media networks. The defendant worked for PhoneDog as a product reviewer and in this role the defendant posted to Twitter his product reviews and blogs to PhoneDog's clients. The Twitter account had 17,000 followers at the time of this action. The defendant left his employ. When the defendant left, PhoneDog requested the defendant to provide the password and cease use of the Twitter account. Instead, the defendant changed the handle for the account and continued to use it. PhoneDog asserted claims for misappropriation of trade secrets, intentional interference with prospective economic advantage, negligent interference with prospective economic damage and conversion. The defendant moved to dismiss the claims against him alleging that the followers did not constitute trade secrets and was publicly available for all to see. However, the court disagreed and ultimately denied all of defendant's motions to dismiss. The court did not specifically address the issue of whether the followers constituted a trade secret. The case then settled in or around January 2013, still leaving the question unanswered as to who owns the content on social media profiles.

- *Christou v. Beatport, LLC*, 849 F. Supp. 2d 1055 (D. Co. Mar. 14, 2012). In *Christou*, the plaintiff owned a host of nightclubs. The defendant Beatport worked for the plaintiff and part of his duties was to maintain the MySpace™ page for the plaintiff's nightclubs. When the defendant opened a competing night club, the defendant allegedly stole the plaintiff's MySpace™ friends in an effort to divert business away from the plaintiff. The plaintiff filed suit against Beatport for theft of its MySpace™ friends, among other claims. The defendant sought to dismiss the claims and argued that the MySpace™ profile and friends did not constitute trade secrets. At the pleading stage, the court disagreed and denied defendant's motion to dismiss because it found that the plaintiff alleged enough facts to maintain the trade secrets claim. The case is currently still pending and awaiting a decision as to whether a MySpace™ profile and friends constitutes a trade secret owned by the employer under Colorado law.

- *Eagle v. Morgan*, 2011 U.S. Dist. LEXIS 147247 (E.D. Pa. Dec. 22, 2011); 2012 U.S. Dist. LEXIS 143614 (E.D. Pa. Oct. 4, 2012). *Eagle* was brought by a former plaintiff CEO of EdComm. When the plaintiff was terminated, the employer accessed the plaintiff's LinkedIn® account that the plaintiff used while employed to promote company business, among other things, changed the password and changed information for the profile to announce the new CEO. The plaintiff brought suit against the employer for federal law violations and numerous state law claims, such as conversion, tortious interference, and other claims, in part due to the employer's access and deprivation to the plaintiff's LinkedIn® account. The employer brought counterclaims against plaintiff alleging conversion, misappropriation, unfair competition, among other claims, based on the plaintiff's use and access to the

LinkedIn® account. The employer argued that the contacts and relationships and related contact information for the LinkedIn® account belonged to the employer. The claims survived motions to dismiss. On October 4, 2012, the court denied summary judgment to the employer on the plaintiff's state law claims and allowed those claims to proceed to trial. The court dismissed the employer's counterclaims with prejudice due to the defendant's failure to follow the time-frames for amending the claims against the plaintiff. The case was tried in November 2012 without a jury; however, post-trial motions are pending and oral argument occurred on February 20, 2013, so the decision on the issues as to the LinkedIn® account still remains undecided.

- 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.

G. PRESERVATION OF SOCIAL MEDIA EVIDENCE

1. **Duty to Preserve**. While there are no published court opinions directly discussing the duties to preserve regarding social media, the courts will likely address this issue in the future. However, a few courts have at least implied that there is a duty to preserve social media and awarded sanctions when the parties failed to preserve such evidence:

   - *Lester v. Allied Concrete Co., supra*, pg. 15 (awarding significant sanctions for lawyer misconduct and spoliation of Facebook® evidence).

   - *Zimmerman v. Weis Markets, Inc*., No. CV-09-1535 (Pa. Ct. Com. Pl. May 19, 2011), the court ordered the "Plaintiff shall not take steps to delete or alter existing information and posts of his MySpace or Facebook accounts."

   - *Howell v. Buckeye Ranch, Inc.,* 2012 U.S. Dist. LEXIS 141368 (S.D. Ohio Oct. 1, 2012) (stating that the plaintiff was on notice that the opposing party was seeking the private information of the plaintiff's social media account once the defendant served discovery requests and the plaintiff has a continuing obligation to preserve the private sections of the plaintiff's social media account).

   - *See also:*

     - *Calvert v. Red Robin Intern., Inc.*, No. C 11-03026 WHA, U.S. Dist. LEXIS 66476 (N.D. Cal. May 11, 2012) (imposing sanctions of over $15,000 on plaintiff for the plaintiff's willful failure to produce certain Facebook® records);

     - *Patel v. Havana Bar, Rest. and Catering*, U.S. Dist. LEXIS 139180 (E.D. Pa. Dec. 5, 2011) (acknowledging that the plaintiff had an affirmative duty to preserve Facebook® witness statements and sanctioning the plaintiff by giving an adverse inference instruction, allowing re-deposition of witnesses at the plaintiff's expense and reasonable attorneys' fees and costs);

- *Torres v. Lexington Ins. Co.*, 237 F.R.D. 533 (D.P.R. 2006) (sanctioning the plaintiff for spoliation of evidence after the plaintiff intentionally deleted web-pages that proved contrary to her claims for emotional damages).

2. **Preservation Required**. In abundance of caution, lawyers should ensure that their clients are doing what they can to preserve social media profiles. Further, there are certain federal agencies that require the preservation of social media, such as FINRA, the SEC and the FDA.[5]

   a. FINRA Regulatory Notice 10-06 (January 2010). With the rise in use of social media networks, FINRA issued this notice with the primary goal to ensure that investors are protected from false or misleading information and that firms are able to effectively supervise staff in the involvement of these sites. The guidance explains firms' record retention requirements when dealing with social media. Specifically, the notice provides that firms that "intend to communicate, or permit its associated persons to communicate, through social media sites must first ensure that it can retain the records of those communications as required by the Securities Exchange Act of 1934." FINRA rules require that a broker-dealer must retain electronic communications that relate to its business. The guidance also explains the duties of firms for supervision of associated persons using or posting to social media sites for business purposes. The entire notice is available at: http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p120779.pdf

   b. SEC. On January 4, 2012, the SEC Office of Compliance Inspections and Examinations issued an alert about the use of social media by investment advisers. For our purposes, the biggest take away from the report was that registered investor advisors have certain record retention obligations under Rule 204-2 of the Investment Advisors Act of 1940 ("IAA"). Under this rule there is no distinction between various types of media that must be preserved. The report advises that investment advisors who use social media must retain records of those communications if the social media content/communications satisfies an investment advisor's recordkeeping obligations under the IAA. It further suggests that advisors determine if it is possible to retain all required records to be in compliance with the IAA. If so, it advises to retain such records in a manner that is easily accessible for a period of not less than five years, and ensure they are available for inspection. *See Investment Adviser Use of Social Media*, SEC Office of Compliance Inspections and Examinations, Vol. II, Issue 1 (January 4, 2012).

   c. FDA. The FDA has numerous record retention policies that impact consumer products in the marketplace. As social media is used more often to promote products, etcetera, the FDA is now faced with the issue of use of social media and its regulatory requirements. In the FDA Reform Act of 2012, Congress required the FDA to issue guidance and regulations on social media, which may likely have some additional requirements. The deadline for the FDA to issue these rules is July 9, 2014.

[5] Financial Industry Regulatory Authority ("FINRA"), U.S. Securities and Exchange Commission ("SEC"), and U.S. Food and Drug Administration ("FDA").

an be stantial ce.

- **Tips and Sources**. Tips for preserving social media evidence, as well as additional sources to refer to on best practices for preserving social media:

  a. Treat social media evidence the same as any other electronically stored information and assume that it is discoverable in litigation.

  b. If you are unsure about how to actually preserve the metadata and embedded materials in social media content, it is wise to consult with IT experts or employ IT personnel that are familiar with the processes for preserving electronically stored information and social media.

  c. Conduct training of staff to educate about the need for record-retention and preservation even of social media profiles and content.

  d. Check to see if the social media network provides for a do-it-yourself function for preserving and saving the social media content. For example, Facebook has a feature called "Download Your Information," which it introduced in October 2010. This feature vows to allow a Facebook® user to download to the user's computer everything the user ever posted to Facebook®, including all messages, posts, pictures, status updates, etcetera. However, it is not advisable for lawyers to rely exclusively on this feature as some experimenting with the program uncovered that this feature does not go back and capture things that have previously been deleted or removed.

  e. For the best practices of preserving electronic evidence, lawyers should refer to *The Sedona Principles: Best Practices Recommendations and Principles Addressing Electronic Document Production*. In addition, for more detailed information and technological assistance on preserving social media, practitioners can refer to the September/October 2011 issue of Information Management, authored by Rakesh Madhava, available at http://content.arma.org/imm/September-October2011/10thingstoknowaboutpreservingsocialmedia.aspx.

H. SOCIAL MEDIA AND ETHICAL ISSUES FOR ATTORNEYS

The following are ethical rules that may be implicated for attorneys when dealing with social media issues:

1. **ABA Mod. R. Prof. Conduct Rule 1.1 Competence (2013):** "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."

- Comment 8. In light of the frequent evolutions in technology, in August 2012, the ABA Commission on Ethics amended the rule on competence to make clear that a lawyer's obligation to keep up on changes in law and practice includes changes to technology and the pro and cons of same. Comment 8 now emphasizes that "a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject."

2. **ABA Mod. R. Prof. Conduct Rule 1.3 Diligence (2013): "**A lawyer shall act with reasonable diligence and promptness in representing a client."

3. **ABA Mod. R. Prof. Conduct Rule 1.6 Confidentiality of Information (2013):** "(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

   - This rule was amended to make it clear to lawyers that they have an ethical obligation to "take reasonable measures to protect" confidential client information and communications from inadvertent disclosure or unauthorized access without regard to the medium.

   - The amended rule delineates factors for lawyers to consider in determining the reasonableness of their safeguards for electronically stored communications and/or confidential client information. These factors include cost of the safeguards and sensitivity of information, while recognizing that all clients and firms are not alike.

   - Significantly, the new rule also makes clear that a lawyer does not violate Model Rule 1.6 merely for unauthorized access to such information by third parties or because of inadvertent disclosures:

     - In the context of social media, lawyers must use caution not to divulge information regarding clients through social media sites, which would violate Rule 1.6.

     - For example, a Texas public defender posted information about her clients on her blog. She was ultimately disbarred for 60 days for violating Rule 1.6, revealing client confidences, under Illinois Rule of Professional Conduct. *See In the Matter of Peshek*, No. 6201779, Comm. No. 09 CH 89 (August 25, 2009).

4. **ABA Mod. R. Prof. Conduct Rule 4.1 Truthfulness in Statements to Others (2013:** "In the course of representing a client a lawyer shall not knowingly: (a) make a false statement of material fact or law to a third person; or (b) fail to disclose a material fact to a third person when disclosure is necessary to avoid assisting a criminal or fraudulent act by a client, unless disclosure is prohibited by Rule 1.6."

5. **ABA Mod. R. Prof. Conduct Rule 4.2 Communication with Person Represented by Counsel (2013):** "In representing a client, a lawyer shall not communicate about the subject of the representation with a person the lawyer knows to be represented by another lawyer in the matter, unless the lawyer has the consent of the other lawyer or is authorized to do so by law or a court order."

   - A lawyer or its legal staff friending an opposing party on Facebook® that the lawyer knows to be represented by counsel could violate Rule 4.2. *See infra, The Philadelphia Bar Ass'n Prof'l Guidance Comm.,* Op. 2009-02 (March 2009); *SDCBA Legal Ethics Opinion 2011-2*.

6. **ABA Mod. R. Prof. Conduct Rule 5.3 Responsibility Regarding Non-Lawyer Assistance (2013):** With respect to a non-lawyer employed or retained by or associated with a lawyer:

> (a) a partner, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer;
>
> (b) a lawyer having direct supervisory authority over the non-lawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and
>
> (c) a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:
>
> (1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or
>
> (2) the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action."

   - The important issue here is that what a lawyer cannot do, a legal assistant or paralegal cannot do. Thus, it would be unethical to ask a paralegal or assistant to "friend" a party whom the lawyer knows to be represented. The same is true for "friending" a person through pre-texting or under false pre-tenses. A lawyer cannot direct a non-lawyer assistant to engage in conduct that would ethically violate the Rules of Professional Conduct.

7. **ABA Mod. R. Prof. Conduct Rule 8.4 Misconduct (2013):** "It is professional misconduct for a lawyer to: …(c) engage in conduct involving dishonesty, fraud, deceit or misrepresentation;"

   - In 2009, the Philadelphia Bar Association's Professional Guidance Committee (the "Committee") issued an opinion regarding an attorney's proposed method of gaining

access to a witness's Facebook® and MySpace™ accounts. The attorney deposed the witness and found out the witness maintained Facebook® and MySpace™ accounts. Believing that the witness might be posting useful information relevant to her deposition on these websites, the attorney visited her Facebook® and MySpace™ accounts and attempted to gain access. However, the attorney discovered that to access the accounts, he would have to "friend" the witness who could then decide whether to grant him access or not. The attorney believed that if he identified himself and asked the witness to "friend" him, she would deny his request. Therefore, the attorney sought the Committee's opinion as to whether the following proposed course of action would violate any ethical rules. The attorney proposed that he would ask a third person, a person whose name the witness would not recognize, to go to her Facebook® and MySpace™ pages and ask her to "friend" him. The person would state only truthful information to the witness, i.e., his real name, but would not reveal that he is affiliated with the attorney. If the witness "friended" the third person, the third person would provide the attorney with the information the witness was posting on her Facebook® and MySpace™ pages. The Committee found that the attorney's proposed course of action could violate various state ethics rules. For example, the Committee found that that proposal could violate Rule 8.4 (Misconduct) because it is inherently deceptive as the plan purposely omits the key fact to the witness that the third party is only seeking to "friend" her so that he can obtain information for the attorney. The Committee found that the proposal could also violate Rule 4.2 (Communication with Person Represented by Counsel), 4.3 (Dealing with Unrepresented Person), Rule 4.1 (Truthfulness in Statements to Others); and 5.3 (Responsibilities Regarding Nonlawyer Assistants). *The Philadelphia Bar Ass'n Prof'l Guidance Comm.*, Op. 2009-02 (March 2009).

- In 2010, in a similar opinion of its own, the New York City Bar Association Committee on Professional Ethics echoed the Philadelphia Committee's opinion, stating that neither attorneys nor their agents were permitted to "friend" potential witnesses under false pre-tenses. The New York City Committee did state however, that lawyers and their agents were permitted to friend request potential witnesses so long as they used only truthful information to obtain the access. The opinion stated, "[a]n attorney or her agent may use her real name and profile to send a 'friend request' to obtain information from an unrepresented person's social networking website[.]"A key distinction between the Philadelphia and New York City Committee opinions is that the New York City opinion states that the lawyer or her agent has no duty to disclose to the party the reasons for making the request. While New York Professional Conduct Rules 4.1 and 8.4(c) are nearly identical to those of Pennsylvania, the New York City Committee finds that the fact that the attorney or his agent seeks information to be used in the course of litigation is not a necessary ethical disclosure. *The Ass'n of the Bar of the City of New York Comm. On Prof. Ethics*, Formal Op. 2010-2 (September 2010).

- Also, in September 2010, the New York State Bar Association issued a second opinion on the issue of whether an attorney can ethically access public social network pages of an opposing party for the purpose of obtaining possible impeachment

evidence for use in litigation. In that opinion, the New York State Bar concluded that there was no ethical issue for an attorney who accesses public social network information that is available to the public domain for viewing. However, the opinion notes that "as long as the lawyer does not 'friend' the other party or direct a third party to do so" there would be no violations of the ethics rules. This analysis is directly in line with its Formal Opinion 2010-2 cited above. *The New York State Bar Ass'n Comm. on Prof. Ethics*, Opin. #843 (September 10, 2010).

- In May 2011, the San Diego County Bar Legal Ethics Committee issued an opinion as to whether an attorney violated the ethical rules when he "friended" two-high ranking employees of the adversary whom his client believed would have negative information about the employer on their social media profiles. The lawyer knew the high-ranking employees were represented by corporate counsel. The opinion found that the lawyer's conduct violated the rules. The opinion went on to note that the rules (Rule 4.2) prohibit the attorney from making an ex parte friend request of a represented party. The committee further found friending an unrepresented third party without disclosing the purpose of the friend request would violate the lawyer's duty not to deceive (Rule 8.4). *SDCBA Legal Ethics Opinion 2011-2.*

- *Oregon State Legal Ethics Comm.*, Formal Ops. 2005-164 (August 2005) and 2005-173 (August 2005). However, the Oregon State Bar seemingly takes a different view on the permissibility of "misrepresentation and subterfuge" by attorneys. In an August 2005 opinion addressing ethically permissible conduct by an attorney with respect to an adversary's website, the Oregon Bar states that information on publicly available websites, or even websites for which a membership or subscription is required, is fair game because it is no different than "reading a magazine article or purchasing a book written by the adversary." The opinion warns, however, that you may not communicate through the Internet with a represented adversary, as doing so would violate a lawyer's ethical duty.

  - Significantly, in footnote 1 of the opinion, the Bar writes, "[w]e express no opinion concerning access to Web sites involving or obtained through the use of deception. *Cf.* OSB Formal Ethics Op No 2005-173."

  - A review of the opinion referenced in footnote 1 shows that the Oregon Bar rules, like the Model Rules, prohibit an attorney from engaging in "conduct involving dishonesty, fraud, deceit or misrepresentation that reflects adversely on the lawyer's fitness to practice law[.]" However, unlike the Model Rules, the Oregon Bar rules further state:

    > [Notwithstanding certain provisions of the Oregon Code] it shall not be professional misconduct for a lawyer to advise clients or others about or to supervise lawful covert activity in the investigation of violations of civil or criminal law or constitutional rights, provided the lawyer's conduct is otherwise in compliance with these Rules of Professional Conduct. **"Covert activity," as used in this rule, means**

an effort to obtain information on unlawful activity through the use of misrepresentations or other subterfuge. "Covert activity" may be commenced by a lawyer or involve a lawyer as an advisor or supervisor only when the lawyer in good faith believes there is a reasonable possibility that unlawful activity has taken place, is taking place or will take place in the foreseeable future.

- The Oregon Bar interprets this to mean that the lawyer must have some rational basis for his belief that an "unlawful activity" has, is or will take place. An "unlawful activity" is defined as "violations of civil law, criminal law, or constitutional rights." Further, it states that civil law "clearly encompasses both statutory and common-law duties, including duties imposed by tort or contract law. 'Civil law' duties regulate both intentional violations and reckless or negligent breaches of civil standards. It is not, however, reasonable to conclude that a 'violation' of 'civil law' refers to a situation in which no breach of any recognized duty is evident or alleged."

- The opinion suggests that, so long as the attorney has a rational basis to believe the investigation relates to unlawful conduct and so long as they do not otherwise violate the Rules of Professional Conduct (for example, by friending a represented party and thereby "communicating" with them in violation of the rules), he or she may use "misrepresentations and subterfuge" to try to obtain informal discovery.

- In August 2012, two New Jersey defense attorneys were charged by the New Jersey Office of Attorney Ethics for violating numerous ethics rules (Rule 4.2, 5.3, 8.4) when their paralegal friended, using her real name, the opposing party who was represented.

8. Miscellaneous Opinions Impacting Electronic Evidence

a. Cloud Computing is Ethically Acceptable. Certain ethic rules are triggered when a lawyer uses cloud computing for storage of client data through third party vendors: Rule 1.1 Competence; Rule 1.6 Confidentiality; and Rule 5.3 Responsibility Regarding Non-Lawyer Assistance. The main concern is client confidentiality and the security of confidential client information on lawyer's files maintained on the cloud.

b. Necessary Precautions. Fourteen states have issued ethics opinions finding that cloud computing or use of similar online backup and file storage is acceptable so long as the lawyers are taking necessary precautions to protect client confidences. These states include:

- Alabama (Opinion 2010-02);
- Arizona (Opinion 09-04);
- California (Opinion 2010-179);
- Florida (Proposed Opinion 12-3);

- Iowa (Opinion 11-01);
- Maine (Opinion 194);
- Massachusetts (Opinion-12-03);
- New Jersey (Opinion 701);
- New York (Opinion 842 and 940);
- Nevada (Opinion 33);
- North Carolina (2011 Formal Ethics Opinion 6);
- Oregon (Opinion 2011-08);
- Pennsylvania (2011-200); and
- Vermont (Opinion 2010-6).

c. The following are a non-exhaustive compilation of suggested measures and safeguards to take to ensure confidentiality:

- Confirming that the third-party vendor has an obligation to preserve confidentiality and security of data;

- Make certain that the providers will notify the lawyer should the provider receive subpoenas or requests requiring disclosure of client information;

- Investigate the providers' security and protocols to determine if the level of security and back up is adequate to protect client confidences;

- Use technology (such as firewalls, virus software, etcetera) to prevent attempts to intrude or steal data;

- Consult an expert if the lawyer is lacking in technology expertise;

- Confirm that the lawyer will have unfettered access to the data;

- Seek an agreement from the vendor or provider to notify the lawyer of breaches; and

- Obtain client approval to store information on the cloud.

I. SPOLIATION AND SANCTIONS FOR DESTRUCTION OF ELECTRONIC EVIDENCE

1. **Sanctions for Use of Cleaners:**

- *Multifeeder Tech. Inc. v. British Confectionary Co.*, 2012 U.S. Dist. LEXIS 132619 (D. Mn. Sept. 18, 2012) (sanctioning party $600,000 based in part on a party's intentional use of CCleaner to clean and wipe computer files).

- *Taylor v. Mitre Corp.*, 2012 U.S. Dist. LEXIS 163854 (E.D. Va. Sept. 10, 2012), *upheld by* 2012 U.S. Dist. LEXIS 161318 (E.D. Va. Nov. 8, 2012) (finding that a plaintiff's use of Evidence Eliminator and CCleaner while in litigation constituted willful spoliation and sanctioned the plaintiff by dismissing the case, awarding fees and costs to the defendant as a result of the spoliation).

- *Ameriwood Indus. Inc. v. Liberman*, 2007 U.S. Dist. LEXIS 74886 (E.D. Mo. July 3, 2007) (awarding default judgment to plaintiff and fees and costs because of defendant's intentional use of "Window Washer" scrubbing software to scrub and/or delete files from computer).;

- *Arista Records, LLC v. Tschirhart*, 241 F.R.D. 462, 466 (W.D. Tex. 2006) (proposed an order of default judgment and awarded fees and costs incurred related to sanctions motion against defendant who willfully destroyed evidence by installing data-wiping software).

- *Communication Center, Inc. v. Hewitt*, 2005 U.S. Dist. LEXIS 10891 (E.D. Cal. April 5, 2005) (recommending default against defendant for use of Evidence Eliminator software and awarding attorneys' fees and costs in the amount of $145,811.75).

- *Kucala Enters. V. Auto Wax Co.*, 2003 U.S. Dist. LEXIS 8833 (N.D. Ill. May 27, 2003) (dismissing plaintiff's lawsuit and awarding defendant attorneys' fees and costs from the date the plaintiff's first use of Evidence Eliminator).

- *But see Coburn v. PN II*, 2010 U.S. Dist. LEXIS 110613 (D. Nev. Sept. 30, 2010) (finding that use of CCleaner alone without other evidence is insufficient to conclude a destruction of evidence occurred).

2. **Standards for Finding Spoliation Sanctions – Negligence vs. Bad Faith.** There is a split between the Circuits on whether "bad faith" or "negligence" is the proper standard.
   a. Bad Faith Required. The Fifth, Seventh, Eighth, Tenth and Eleventh and D.C. Circuits require "bad faith" before providing a serious spoliation sanction such as an adverse jury instruction:

      - *Rimkus*, 2010 WL 645253, *6-7 (S.D. Tex. 2010)

      - *See Faas v. Sears, Roebuck, & Co*, 532 F.3d 633, 644 (7th Cir. 2008) (requiring finding that Sears intentionally destroyed documents in bad faith before drawing an inference that the documents contained information detrimental to Sears).

      - *Greyhound Lines v. Wade*, 485 F.3d 1032, 1035 (8th Cir. 2007) (a spoliation-of-evidence sanction requires a finding of intentional destruction indicating a desire to suppress the truth).

      - *Turner v. Pub. Serv. Co. of Colo.*, 563 F.3d 1136, 1149 (10th Cir. 2009) (mere negligence in losing or destroying records is not enough because it does not

support an inference of consciousness of a weak case).

- *Penalty Kick Mgmt. Ltd. v. Coca Cola Co.*, 318 F.3d 1284, 1294 (11th Cir. 2003) ("adverse inference is drawn from a party's failure to preserve evidence only when the absence of that evidence is predicated on bad faith").

- *Wyler v. Korean Air Lines Co.*, 928 F.2d 1167, 1174 (D.C. Cir. 1991) ("Mere innuendo…does not justify drawing the adverse inference requested").

b. Bad Faith Not Essential. The First, Fourth, and Ninth Circuits hold that "bad faith" is not essential to imposing severe sanctions if the spoliation causes severe prejudice to a party's ability to prove its case, but the cases often note the presence of bad faith:

- *Rimkus* at *7 fn. 12.

- *See Sacramona v. Bridgestone/Firestone, Inc.*, 106 F.3d 444, 447 (1st Cir. 1997) (bad faith may be considered but is not essential for sanction regarding spoliation; if evidence is mishandled through carelessness and other side is prejudiced, sanctions may be imposed).

- *Silvestri v. Gen. Motors Corp.*, 271 F. 3d 583, 593 (4th Cir. 2001) (holding dismissal is "usually justified only in circumstances of bad faith, but even when conduct is less culpable, dismissal may be necessary if prejudice to defendant is extraordinary, denying it the ability to adequately defend its case).

- *Glover v. BIC Corp.*, 6 F. 3d 1318, 1329 (9th Cir. 1993) ("Short of excluding the disputed evidence, a trial court also has the broad discretionary power to permit a jury to draw an adverse inference from the destruction or spoliation against the party or witness responsible for the behavior").

c. Balance. The Third Circuit courts balance the degree of fault with the prejudice before applying spoliation sanctions. *Rimkus at 7 fn. 13.*

- *See Mosaid Techs. Inc., v. Samsung Elecs, Co.*, 348 F.Supp.2d 332, 335 (D. N.J. 2004) (three key considerations dictate if sanctions are warranted: (1) degree of fault of the party who altered or destroyed evidence, (2) degree of prejudice suffered by opposing party, and (3) whether there is a lesser sanction that will avoid unfairness to opposing party and serve to deter such conduct by others in the future) (citing *Schmid v. Milwaukee Elec. Tool Corp.*, 13 F.3d 76, 79 (3d Cir. 1994).

3. **Range Of Penalties for Spoliation of Evidence.**

a. Sanctions. Courts have used a wide variety of sanctions in response to e-discovery violations: evidence preclusion, witness preclusion, disallowance of certain defenses, reduced burden of proof, removal of jury challenges, limiting closing statements,

supplemental discovery, additional access to computer systems, payments to bar associations to fund educational programs, participation in court-created ethics programs, referrals to the state bar, payments to the clerk of court, and barring the sanctioned party from taking additional depositions.[6]

b. Additional sanctions include:

(1) Monetary Sanctions;

- *See Lester v. Allied Concrete Co.*, 83 Va. Cir. 308, 2011 Va. Cir. LEXIS 245 (Sept. 2011); 83 Va. Cir. 308, 2011 Va. Cir. LEXIS 132 (Oct. 2011). (Sanctioning attorney and attorney's client in the amount of $720,000 for lawyer's instruction to clean-up Facebook® page and client's subsequent spoliation of Facebook® photos).

(2) Exclusion of Expert Testimony;

(3) Adverse Inference Jury Instruction;

(4) Dismissal of Offending Party's Claim

(5) Default Judgment Against Offending Party

(6) Imprisonment

J. INVASION OF PRIVACY AND ACCESSING SOCIAL MEDIA

1. **Right to Privacy Issue**. Privacy is becoming a big issue as the number of users of social media rises daily. Essentially, there are three areas of law attorneys should be looking to determine if improper access of social media or discovery of social media gives rise to invasion of privacy type of claims. These legal principles lie in constitutional protections, statutory protections and common law protections. The central issue is whether an individual has a right to privacy or a cause of action for such invasions of privacy in the context of his or her social media accounts. However, social media and privacy is a whole other topic. For our purposes, the point is to make practitioners aware of the potential legal issues that can develop from the use of social media.

2. **Expectation of Privacy**. To determine whether a client has an expectation of privacy or can bring a constitutional, statutory or common law claim for invasion of privacy for unauthorized access to an individual's social media profile, practitioners should look to the following sources:

a. Constitutional Protections:

[6] Dan H. Willoughby, Jr., Rose Hunter Jones, and Gregory R. Antine, *Sanctions for E-discovery Violations: By the Numbers*, Duke Law Journal, 60 Duke L.J. 789 (December 2010)

- First Amendment
- Fourth Amendment
- Fifth Amendment
- Ninth and Fourteenth Amendment

b. Statutory Protections:

- Electronic Communications Privacy Act a/k/a the Federal Wiretap Act
- The Stored Communications Act
- State Laws on Prohibited Access to Social Media, *supra* Section A.
- State Off-Duty Conduct Statutes

c. Common Law Torts.

K. ON THE HORIZON – NEW DEVELOPMENTS IN SOCIAL MEDIA THAT ATTORNEYS SHOULD KNOW

1. **Twitter Interviews.** Twitter interviews are the hot trend right now where employers post questions on Twitter for followers to answer and employers to use responses to weed through applicants. At first blush, it does not appear that using Twitter for interviews would automatically trigger any ethical or other concerns. However, using Twitter for interviews of potential job candidates will invoke an employer's obligation to retain and preserve employment records as required by the EEOC and ensure that such Twitter interviews are preserved in anticipation of litigation.

2. **Competitive Intelligence Information**. Competitive intelligence specialists are trained to scour the Internet to obtain information about a business' competitors. Because employees use social media to post about work-related issues, these specialists are able to obtain insight about a company's recent faults and successes, potential mergers and acquisitions, or upcoming products, services or solutions a company is about to launch. Professional websites such as LinkedIn® are also prime places for headhunters and competitors to research the competition, scout an organization's top talent, and obtain their contact information in order to try to steal them away. It is uncertain what ethical considerations will arise out of this new technology, but lawyers should at least be vigilant regarding the new technologies that may impact their practice or cases.

L. DISCOVERY OF ELECTRONIC EVIDENCE

1. **Cases Allowing Discovery of Information from Social Networking Websites:**

- *Reid v. Ingerman Smith LLP*, 2012 U.S. Dist. LEXIS 182439 (E.D.N.Y. Dec. 27, 2012) (ordering plaintiff to disclose social media content and photographs relevant to claims for emotional damages for certain time period).

- *E.E.O.C. v. Honeybaked Ham Co. of Ga.*, 2012 U.S. Dist. LEXIS 160285 (D. Co. Nov. 7, 2012) (compelling disclosure of each class member's social media, subject to process delineated by court).

- *Robinson v. Jones Lang Lasalle Americas, Inc.*, 2012 U.S. Dist. LEXIS 123883 (D. Or. Aug. 29, 2012) (compelling plaintiff to produce social media content relevant to plaintiff's emotional distress damages and/or emotional, feeling or mental state).

- *Coates v. Mystic Blue Cruises, Inc., et al.*, 2012 U.S. Dist. LEXIS 112011 (N.D. Ill. Aug. 9, 2012) (sexual harassment case, allowing discovery of plaintiff's Facebook® messages with co-workers where the messages revealed intimate conversations between the plaintiff and certain male employees).

- *Targonski v. City of Oak Ridge*, 2012 U.S. Dist. LEXIS 99693 (E.D.T.N. July 18, 2012 (noting that jury could consider plaintiff's Facebook® evidence in deciding sexual harassment, disparate treatment and retaliation claims)

- *Davenport v. State Farm Mut. Auto. Ins. Co.*, 2012 U.S. Dist. LEXIS 20944 (M.D. Fla. Feb. 21, 2012) (granting defendant's motion to compel plaintiff's Facebook® photos, but denying access to plaintiff's electronic devices to access plaintiff's social media profiles).

- *Offenback v. L.M. Bowman, Inc.*, 2011 U.S. Dist. LEXIS 66432 (M.D. Pa. June 22, 2011) (after in camera review compelling limited production of plaintiff's Facebook® material relevant to plaintiff's claims).

- *Held v. Ferrellgas, Inc.*, 2011 WL 3896513 (D. Kan. Aug. 31, 2011) (compelling content from plaintiff's Facebook® account relevant to plaintiff's retaliation claims).

- *Holter v. Wells Fargo and Co.*, 281 F.R.D. 340 (D. Mn. May 4, 2011) (compelling production of plaintiff's Facebook® content relevant to issue of emotional damages, plaintiff's employment with defendant and plaintiff's work search efforts, but refusing to compel plaintiff to provide defendant social media passwords giving unfettered access to defendant).

- *Equal Employment Opportunity Commission v. Simply Storage Management*, Discovery Order Issued on May 11, 2010, Case No. 1:09-cv-1223-WTL-DML (S.D. Ind. 2010) (compelling Facebook® content relevant to lawsuit and claim for emotional damages). *Simply Storage* is considered the seminal, leading case on the discovery of social media.

- *Ledbetter v. Wal-Mart Stores, Inc.*, 2009 WL 1067018 (D. Colo. 2009) (allowing subpoenas to Facebook®, MySpace™ and other social media sites because the plaintiff's claims for physical and psychological injuries and loss of consortium made the issues the subpoenas were aimed at finding relevant)

- *Bass v. Miss Porter's School*, 2009 WL 3724968 (D. Conn. 2009) (granting access to student's Facebook® posts and messages).

2. **Cases Denying Discovery of Information from Social Networking Websites:**

- *Howell v. Buckeye Ranch, Inc.*, No. 2-11-cv-1014 (S.D. Ohio Oct. 1, 2012) (denying motion to compel plaintiff's Facebook® username and password noting that granting such a request would give the defendant unfettered access regardless of relevance).

- *Tompkins v. Detroit Metro. Airport*, (E.D. Mich. Jan. 18, 2012) (denying defendant's request for plaintiff's release of Facebook® content where defendant could not make a sufficient predicate showing that the material was relevant).

- *Debord v. Mercy Health System of Kansas, Inc.*, 2011 U.S. Dist. LEXIS 87019 (Aug. 8, 2011) (denying motion to compel Facebook® content posted after the plaintiff's termination because the postings could not have formed the basis for the plaintiff's termination).

- *Muniz v. United Parcel Service*, 2011 U.S. Dist. LEXIS 11219 (Jan. 28, 2011) (quashing subpoena for postings to listservs and social media networks because the information sought was not relevant in fee dispute).

- *Mackelprang v. Fidelity National Title Agency of Nevada, Inc.*, 2007 WL 119149 (D. Nev. 2007) (denying employer's unfettered access to all private content of plaintiff's MySpace™ page, but allowing the defendant to submit requests for production for Mackelprang's MySpace™ pages relevant to claims for emotional damages).

APPENDIX A

Employer Access to Social Media Usernames and Passwords 2013

Increasing numbers of Americans use social media both on and off the job. Recently, some employers have asked employees to turn over their usernames or passwords for their personal accounts. Some employers argue that access to personal accounts is needed to protect proprietary information or trade secrets, to comply with federal financial regulations, or to prevent the employer from being exposed to legal liabilities. But others consider requiring access to personal accounts an invasion of employee privacy.

State lawmakers introduced legislation beginning in 2012 to prevent employers from requesting passwords to personal Internet accounts—including email, banking and social networking sites—to get or keep a job. Some states have similar legislation to protect students in public colleges and universities from having to grant access to their social networking accounts.

NCSL Resources

2012 Legislation: Employer Access to Social Media Usernames and Passwords

Telecommunications and Information Technology

NCSL Contact

Pam Greenberg, Denver Office

2013 Legislation

As of Feb. 15, 2013

Legislation has been introduced or is pending in at least 28 states in 2013. *(See also 2012 legislation.)*

Arizona
S.B. 1411
Status: Feb. 5, 2013; To Senate Committees on Commerce and Energy, Public Safety, Rules.
Relates to social media passwords; relates to prohibition.

California
A.B. 25
Status: Jan. 24, 2013; To Assembly Committees on Judiciary and Public Employees, Retirement and Social Security.
Existing law prohibits a private employer from requiring or requesting an employee or applicant for employment to disclose a username or password for the purpose of accessing personal social media, to access personal social media in the presence of the employer, or to divulge any personal social media. Existing law prohibits a private employer from discharging, disciplining, threatening to discharge or discipline, or otherwise retaliating against an employee or applicant for not complying with a request or demand that violates these provisions. This bill would apply the provisions described above to public employers. The bill would state that its provisions address a matter of statewide interest and apply to public employers generally, including charter cities and counties.

Colorado
H.B. 1046
Status: Jan. 12, 2013; To House Committee on Appropriations.
Concerns employer access to personal information through electronic communication devices.

Connecticut
H.B. 5690
Status: Jan. 23, 2013; To Joint Committee on Labor and Public Employees.
Prohibits employers from requesting access to their employees' personal social media accounts; protects employee privacy by barring employers or potential employers from requiring employees to provide passwords to their personal accounts as a condition of employment.

S.B. 159
Status: Jan. 13, 2013; To Joint Committee on Labor and Public Employees.
Concerns employee privacy; protects employee privacy by barring employers or potential employers from requiring employees to provide passwords to their personal accounts as a condition of employment.

Georgia
H.B. 117
Status: Jan. 29, 2013; To House Committee on Industry and Labor.
Prohibits employers from requesting username, password, or other means of accessing an account or service for the purpose of accessing personal social media through an electronic communications device of employees or prospective employees with certain exceptions, provides for penalties, provides for related matters, repeals conflicting laws.

H.B. 149
Status: Jan. 31, 2013; To House Committee on Industry and Labor.
Prohibits employers from requesting or requiring that an employee or applicant for employment disclose a username or password for the purpose of accessing personal social media, prohibits employers from requesting or requiring that an employee or applicant access personal social media in the presence of the employer, prohibits an employer from taking adverse action against an employee or applicant for employment for not complying with such a request or demand, provides for definitions.

Hawaii
H.B. 713
Status: Feb. 12, 2013; In House Committee on Judiciary: Hearing Scheduled.
Prohibits employers from requiring employees and applicants for employment from disclosing social media usernames or passwords.

H.B. 1023
Status: Jan. 22, 2013; Introduced.
Prohibits educational institutions and employers from requesting a student, prospective student employee, or prospective employee to grant access to, allow observation of, or disclose information that allows access to or observation of personal internet accounts; provides penalties.

S.B. 207
Status: Feb. 12, 2013; In Senate Committee on Technology and the Arts: Voted do pass with amendment.
Prohibits employers from requiring employees and applicants for employment from disclosing social media usernames or passwords.

Illinois
H.B. 64
Status: Jan. 9, 2013; To House Committee on Rules.
Creates the Privacy in the School Setting Act. Defines "school" as an institution of higher learning as defined in the Higher Education Student Assistance Act, a public elementary or secondary school or school district, or a nonpublic school recognized by the State Board of Education. Provides that it is unlawful for a school to request or require a student or prospective student or his or her parent or guardian to provide a password or other related account information in order to gain access to the student's or prospective student's account or profile on a social networking website or to demand access in any manner to a student's or prospective student's account or profile on a social networking website.

H.B. 851
Status: Jan. 25, 2013; To House Committee on Rules.
Amends the Right to Privacy in the Workplace Act; makes a technical change in a Section concerning prohibited inquiries.

H.B. 1047
Status: Jan. 30, 2013; To House Committee on Rules.
Amends provisions of the Right to Privacy in the Workplace Act prohibiting certain inquiries by an employer; deletes language in those provisions regarding an employee's social networking website account information; provides that: an employer may not request or require an employee or prospective employee to provide a user name, password, or other means to gain access to the employee's or prospective employee's personal online account.

S.B. 2306
Status: Feb. 15, 2013; In Senate Committee on Assignments.
Amends the Right to Privacy in the Workplace Act; provides that the restriction on an employer's request for information concerning an employee's social networking profile or website applies to only the employee's personal account; defines terms; provides that employers are not prohibited from complying with the rules of self-regulatory organizations.

Iowa
H.F. 127
Status: Feb. 4, 2013; To House Committee on Education
Prohibits employers and schools from seeking access to certain online personal employee and student information and providing penalties.

Kansas
H.B. 2092
Status: Jan. 25, 2013; To House Committee on Commerce, Labor and Economic Development
Relates to prohibiting employers from requiring employees to divulge social media content.

H.B. 2094
Status: Jan. 25, 2013; To House Committee on Education.
Relates to student electronic privacy at public and private postsecondary educational institutions.

S.B. 53
Status: Jan. 22, 2013; To Senate Committee on Commerce.
Prohibits employers from requiring employees to divulge social media content.

Maine
L.R. 20
Status: Jan. 28, 2013; Filed.
Protects social media privacy in school and the workplace.

L.R. 1011
Status: Jan. 28, 2013; Filed
Protects employee social media privacy.

Maryland
H.B. 1332
Status: Feb. 8, 2013; To House Committee on Appropriations.
Relates to educational institutions; relates to personal electronic account; relates to privacy protections.

S.B. 838
Status: Feb. 6, 2013; To Senate Committee on Rules.
Prohibits an educational institution from requiring, requesting, suggesting, or causing a student, an applicant, or a prospective student to grant access to, allow observation of, or disclose information that allows access to or observation of the individual's personal electronic account; prohibits an educational institution from compelling, as a condition of acceptance or participation in specified activities, an individual to add specified individuals to a list of contacts or to change privacy settings.

Massachusetts
H.D. 503
Status: Jan. 15, 2013; Introduced.

Relates to social network privacy and employment.

Minnesota

H.F. 293
Status: Feb. 4, 2013; To House Committee on Labor, Workplace and Regulated Industries
Relates to employment; prohibits employers from requiring social network passwords as a condition of employment.

H.F. 611
Status: Feb. 14, 2013; To House Committee on Labor, Workplace and Regulated Industries
Relates to employment; prohibits prohibiting employers from requiring social network passwords as a condition of employment.

S.F. 484
Status: Feb. 14, 2013; To Senate Committee on Jobs, Agriculture and Rural Development.
Relates to employment; prohibits employers from requiring social network passwords as a condition of employment.

S.F. 596
Status: Feb. 20, 2013; Introduced.
Relates to employment; prohibits employers from requiring social network passwords as a condition of employment.

Mississippi

H.B. 165
Status: Feb. 5, 2013; Died in Committee.
Prohibits employers from obtaining passwords or other account information to gain access to social networking sites of employees and prospective employees; provides penalties for violations.

Missouri

H.B. 115
Status: Jan. 9, 2013; Introduced.
Prevents repercussions on employees or prospective employees for failure to disclose private information to the employer.

H.B. 286
Jan. 23, 2013; Introduced.
Prohibits employers from asking current or prospective employees to provide certain information to gain access to a social networking website where such employees maintain an account or profile.

S.B. 164
Status: Jan. 17, 2013; Introduced.
Protects employees from being required to disclose personal user names or passwords.

Montana

S.B. 195
Status: Feb. 13, 2013; From Senate Committee on Judiciary: Do pass as amended
Revises laws protecting job applicant and employee privacy related to social media; relates to labor and employment; relates to privacy.

Nebraska

L.B. 58
Status: Jan. 14, 2013; To Legislative Committee on Business and Labor.
Adopts the Workplace Privacy Act.

New Hampshire

H.B. 379
Status: Jan. 3, 2013; To House Committee on Labor, Industrial and Rehabilitative Services. Filed as LSR 82,
Prohibits an employer from requiring a prospective employee to disclose his or her social media passwords.

H.B. 414
Status: Jan. 22, 2013; To House Committee on Labor, Industrial and Rehabilitative Services. Filed as LSR 505.
Prohibits an employer from requiring an employee or prospective employee to disclose his or her social media passwords.

New Jersey

A.B. 2878
Status: Nov. 12, 2012; Passed Senate. Received in the Assembly, 2nd Reading on Concurrence.
Prohibits requirement to disclose user name, password, or other means for accessing account or service through electronic communications device by employers.

S.B. 1898
Status: Sept. 20, 2012. From Senate Committee on Labor as combined. For further action see S.B. 1915.
Prohibits requirement to provide information for access to account on social networking website by employer.

S.B. 1915
Status: Oct. 25, 2012; Substituted by A2878.
Prohibits requirement to disclose user name, password, or other means for accessing account or service through electronic communications device by employers.

New Mexico

S.B. 371
Status: Jan. 31, 2013; To Senate Committee on Judiciary.
Relates to employment; prohibits prospective employers from requesting or requiring a prospective employee to provide a password or access to the prospective employee's social networking account.

S.B. 422
Feb. 5, 2013; To Senate Committee on Judiciary.

Relates to education; prohibits public and private institutions of post-secondary education from requesting or requiring a student, applicant or potential applicant for admission to provide a password or access to the social networking account of the student or applicant for admission.

New York

A.B. 443

Status: Jan. 9, 2013; To Assembly Committee on Labor.

Prohibits an employer from requesting that an employee or applicant disclose any means for accessing an electronic personal account or service.

S.B. 1701

Status: Jan. 9, 2013; To Senate Committee on Labor.

Protects the privacy of employees' and prospective employees' social media accounts.

S.B. 2434

Status: Jan. 17, 2013; To Senate Committee on Labor.

Prohibits an employer from requesting or requiring that an employee or applicant disclose any user name, password, or other means for accessing a personal account or service through specified electronic communications devices.

North Dakota

H.B. 1455

Status: Feb. 8, 2013; Passed House; To Senate.

Relates to internet accounts and workplace privacy of social media accounts.

Oregon

H.B. 2654

Status: Jan. 14, 2013; Introduced.

Prohibits employer from compelling employee or applicant for employment to provide access to personal social media account or to add employer to social media contact list; prohibits retaliation by employer against employee or applicant for refusal to provide access to accounts or to add employer to contact list; prohibits certain educational institutions from compelling student or prospective student to provide access to personal social media account.

S.B. 344

Status: Jan. 14, 2013; Introduced.

Establishes unlawful employment practice for certain actions taken by employer to access employee's or prospective employee's personal account on social networking website for employment purposes; declares emergency, effective on passage.

S.B. 499

Status: Feb. 6, 2013; Introduced.

Prohibits an employer from compelling an employee or applicant for employment to provide access to personal social media account or to add employer to social media contact list; prohibits retaliation by employer against employee or applicant for refusal to provide access to accounts or to add employer to contact list; prohibits certain educational institutions from compelling student to provide access to personal social media account; relates to coaches, teachers, administrators and other employees.

Rhode Island

H.B. 5255

Status: Feb. 5, 2013; To House Committee on Judiciary.

Establishes a social media privacy policy for students and employees.

Texas

H.B. 318

Status: Jan. 8, 2013; Introduced.

Relates to prohibiting an employer from requiring or requesting access to the personal accounts of employees and job applicants through electronic communication devices; establishes an unlawful employment practice.

H.B. 451

Status: Jan. 10, 2013; Introduced.

Relates to restrictions on access to certain personal online accounts through electronic communication devices by employers or public or private institutions of higher education. Establishes an unlawful employment practice.

S.B. 118

Status: Jan. 8, 2013; Introduced.

Prohibits an employer from requiring or requesting access to the personal accounts of employees and job applicants through electronic communication devices; establishing an unlawful employment practice.

S.B. 416

Status: Status: Feb. 7, 2013; Introduced.

Relates to restrictions on access to certain personal online accounts through electronic communication devices by employers or public or private institutions of higher education; establishes an unlawful employment practice.

Utah

H.B. 100

Status: Feb. 12, 2013; From House Committee on Public Utilities and Technology: Reported favorably as amended.

Modifies provisions addressing labor in general and higher education to enact protections for personal Internet accounts; enacts the Internet Employment Privacy Act, including defining terms, permitting or prohibiting certain actions by an employer; provides that the chapter does not create certain duties; provides private right of action; enacts the Internet Postsecondary Education Privacy Act.

Vermont

S.B. 7

Jan. 11, 2013; To Senate Committee on Economic Development, Housing and General Affairs.

Relates to social networking privacy protection.

Washington

S.B. 5211

Status: Jan. 23, 2013; To Senate Committee on Commerce and Labor.

Concerns social networking accounts and profiles.

Denver Office
Tel: 303-364-7700 | Fax: 303-364-7800 | 7700 East First Place | Denver, CO 80230

Washington Office
Tel: 202-624-5400 | Fax: 202-737-1069 | 444 North Capitol Street, N.W., Suite 515 | Washington, D.C. 20001