SEYFARTH SHAW

Social Media Privacy Legislation

What Employers Need to Know Desktop Reference

2017–2018 EDITION

Social media and related issues in the workplace can be a headache for employers. Seyfarth Shaw LLP's Social Media Practice Group is pleased to provide you with an easy-to-use guide to social media privacy legislation and what employers need to know. The Social Media Privacy Legislation Desktop Reference:

- Describes the content and purpose of the various states' social media privacy laws.
- Delivers a detailed state-by-state description of each law, listing a general overview, what is prohibited, what is allowed, the remedies for violations, and special notes for each state.
- Provides an easy-to-use chart listing the states that have enacted social media privacy laws and the features of the law in all such states.
- Offers our thoughts on the implications of this legislation in other areas, including trade secret misappropriation, bring your own device issues and concerns, social media discovery and evidence considerations, and use of social media in internal investigations.
- Concludes with some best practices to assist companies in navigating this challenging area.

Table of Contents

Dear Clients and Friends

We are pleased to provide you with the 2017–2018 edition of our *Social Media Privacy Legislation Desktop Reference: What Employers Need to Know.* There is no doubt that social media has transformed the way that companies conduct business. In light of the rapid evolution of social media, companies today face significant legal challenges on a variety of issues ranging from employee privacy and protected activity to data practices, identity theft, cyber security, and protection of intellectual property.

Over the past year, the District of Columbia, Nebraska, Vermont, and West Virginia have joined a growing number of states in enacting social media privacy laws regulating the use of social media by employers and educational institutions. In addition, over the past several years employee use of social media has increasingly generated disputes in trade secrets and non-compete litigation, while employer policies regarding employee use of social media have attracted the attention of the National Labor Relations Board and other federal and state regulatory agencies.

Given the increasing pervasiveness of social media in the workforce, employers need to stay informed of the varied and ever-evolving legal requirements governing employee use of social media. To provide a starting point for that analysis, we have created this convenient, one-stop Desktop Reference surveying existing social media privacy laws. This Desktop Reference delivers a detailed state-by-state description of various states' social media privacy laws, provides an easy-to-use chart summarizing the key features of these laws, and offers our thoughts on the implications of this legislation in other areas, including technological advances in the workplace, trade secret misappropriation, bring your own device issues and concerns, social media discovery, and other implications. Of course, the information contained in this booklet is understandably condensed and simplified, and thus, while it provides a convenient point of reference, always consult with your attorney before making any decisions.

Keeping abreast of the latest developments is also one of our top priorities. We invite you to visit our ABA Top 100 award-winning blog, Trading Secrets, at www.tradesecretslaw.com for commentary and analysis on hot new topics in the world of social media law, trade secrets, privacy, non-competes, unfair competition, and computer fraud.

We hope this booklet provides a useful and informative tool. Please do not hesitate to contact a Seyfarth Shaw Trade Secrets attorney if you have any questions.

Robert B. Milligan

Los Angeles Partner,
Social Media Practice Group

Daniel P. Hart

Atlanta Partner,
Social Media Practice Group

Introduction

Social media privacy issues now permeate the workplace. Since April 2012, a growing number of states have enacted social media privacy laws regulating the use of social media by employers and educational institutions. The various laws, in varying degrees, prohibit employers and/or higher education institutions from requesting or requiring employees, prospective employees, students, or applicants to provide access to their social media accounts (i.e. Facebook, Twitter, LinkedIn, WhatsApp, SnapChat, Yelp, Vine, Pinterest, Instagram, Tumblr, etc.), whether through username/password disclosure, opening the accounts in a boss's presence, adding an employer representative to a contact list, or altering the account's privacy settings. Many of the laws (though not all) allow those employees or students whose rights have been violated to file lawsuits, or complaints with state agencies, for money damages, penalties, injunctions, attorneys' fees, or other forms of relief. One law makes it a misdemeanor for an employer to violate these newly established statutory privacy rights.

Nevertheless, most social media privacy laws contain a number of exceptions and safe harbors for the benefit of employers and schools. Many of the statutes prohibit requested or required access only to personal social networking accounts—those which employees do not use for employer business, or which, if applicable, students do not use for academic purposes. Many of the laws also allow account access during the course of investigations of employment-related misconduct or theft of employer data, or to permit access to employer-owned equipment or information systems. Some of the laws also permit mandatory access to accounts for required self-regulatory employee screening, such as broker screening under NASD and FINRA rules. Still other provisions provide immunity to employers for "innocent discovery" of protected information during ordinary network monitoring. Some laws also provide immunity to employers who decline or fail to demand access to protected accounts, even when such access is arguably permitted by statute.

So far, few, if any, court decisions have interpreted any of the new social media privacy laws. In the future, we anticipate that courts will be asked to address issues related to: (1) what constitutes a personal vs. non-personal account, especially in those states whose laws do not define those terms; (2) the permissible scope of employer investigations involving mandatory access to employee accounts; (3) the implications of the privacy laws for employers' trade secrets, including employer vs. employee ownership of social media account-related information, and sufficient secrecy measures in light of the mandatory-access prohibitions and exceptions; (4) discovery disputes involving social networking account content; (5) the privacy laws' implications on the Computer Fraud and Abuse Act and other state and federal laws; and (6) other implications of the privacy laws.

State-By-State Survey

1. Arkansas

Statutes: Codified at ARK. CODE ANN. § 11-2-124 (2017) (employers); ARK. CODE ANN. § 6-60-104 (2013) (educational institutions).

General overview: Governor Beebe signed the educational bill on April 8, 2013 and signed the employer bill on April 22, 2013. Both laws were effective immediately. The employer law was amended on April 1, 2017.

What's prohibited: (i) the requested or required (1) turnover of account login; or (2) privacy-settings changes for employee and applicant personal accounts; and (ii) the required adding of employer to contacts list. Retaliation against employee or rejection of applicant for refusal is also prohibited.

What's allowed: viewing publicly available information about an applicant or employee. Mandatory account access for accounts which were (1) opened at employer's request; (2) provided by the employer; (3) set up on employer's behalf; and (4) set up to impersonate employer. Also, mandatory access is permitted for good-faith investigation into illegal conduct or breach of written employer policy.

What's the remedy: civil penalties or criminal misdemeanor fines of between $10 – $100 for each violation; no private civil action authorized.

Special notes: effectively defines personal accounts as those different from the accounts to which employers may require access. Contains "innocent discovery" shield for employers that inadvertently learn protected account login information through employer-owned devices or employer network-monitoring.

2. California

Statutes: Codified at CAL. LAB. CODE § 980 (2012) (employers); CAL. EDUC. CODE § 99121 (2012) (educational institutions).

General overview: On September 27, 2012, Governor Brown signed Assembly Bill 1844, which regulates employers' ability to demand access to employees' or prospective hires' personal social media accounts. The law went into effect on October 1, 2012.

What's prohibited: the requested or required (i) turnover of account login; (ii) employer access; and (iii) disclosure of account content for employee, applicant, or student personal accounts. Retaliation against employee or rejection of applicant for refusal is also prohibited.

What's allowed: reasonable-belief investigation into employee misconduct (use of the information is limited to that investigation); mandatory login turnover to access employer-owned devices.

What's the remedy: possible PAGA claims or Bus. & Prof. Code § 17200 claims.

Special notes: no definition of personal account; no mandatory Labor Commission investigation or enforcement of alleged violations.

3. Colorado

Statute: Codified at COLO. REV. STAT. § 8-2-127 (2013).

General overview: Governor Hickenlooper signed the bill on May 11, 2013, and it became effective immediately.

What's prohibited: the requested or required (i) turnover of account login; (ii) employer access; (iii) adding employer to contacts list; and (iv) privacy settings changes for employee and applicant personal accounts. Retaliation against employee or rejection of applicant for refusal is also prohibited.

What's allowed: mandatory turnover of non-personal account login; information-based investigations of personal account activity raising issues of (i) compliance with securities or financial law or regulations; or (ii) of employee theft of employer's proprietary assets. Enforcement of personnel policies not in conflict with the statute is also permitted.

What's the remedy: complaints to Dept. of Labor and Employment; fines up to $1,000 for first violation and up to $5,000 for each subsequent violation; no civil action authorized.

Special notes: no definition of personal or non-personal account. The statute clarifies that it does not permit employee disclosure of employer confidential information. There is an exception for law enforcement positions.

4. Connecticut

Statute: Codified at CONN. GEN. STAT. § 31-40x (2015).

General overview: Governor Malloy signed Public Act 15-6 on May 19, 2015, and it went into effect on October 1, 2015.

What's prohibited: the requested or required (i) turnover of account login; (ii) employer authentication or access in the presence of employee; and (iii) adding of employer to contacts list for employee and applicant personal accounts. Discharge, discipline, and retaliation against an employee or applicant for refusal is prohibited.

What's allowed: an employer may request or require turnover of employee or applicant login for (i) any employer provided account; or (ii) any account used for business purposes. Employer may discipline or discharge an employee that transfers proprietary information through a personal account. Employer may also require access to a personal account to investigate a violation of state or federal law or transfer of proprietary information, but may not request the turnover of a user name or password.

What's the remedy: complaints to the Labor Commissioner, award of attorneys' fees for prevailing employee, civil penalties up to $500 for first violation and $1,000 for each subsequent violation, employee rehire, payment of back wages, reinstatement of employee benefits.

Special notes: exception for law enforcement positions.

5. Delaware

Statutes: Codified at DEL. CODE ANN. tit. 19, § 709A (2015) (employers); DEL. CODE ANN. tit. 14, §§ 8101-8105 (2012) (educational institutions).

General overview: Governor Markell signed the educational institution bill on July 20, 2012, and the employer bill on August 7, 2015, and both became effective immediately.

What's prohibited: the requested or required (i) turnover of account login; (ii) institution direct or indirect access; (iii) access in the presence of the employer; (iv) conditioning employment upon use of social media; (v) adding employer or representative to contacts list; and (vi) altering of privacy settings. Institution tracking of student or applicant account activity, and disciplining student and rejecting applicant for refusals are also prohibited.

What's allowed: institution's public-safety or police department's investigation of suspected criminal activity, or an investigation per institution's threat assessment policy or protocol. Compliance with personnel policies and law, accessing employer-provided accounts, and monitoring use on the employer's network is permitted.

What's the remedy: unclear. The statute itself provides none. No enforcement or remedies provisions are readily ascertainable.

Special notes: exception for law enforcement positions.

6. District of Columbia

Statute: Codified at D.C. CODE §§ 38-831.01-.05 (2017).

General overview: Mayor Bowser signed the bill on December 21, 2016, and it became effective on February 18, 2017, with text of §§ 38-831.02-.04 to become applicable on August 1, 2017.

What's prohibited: the required (i) turnover of account login; (ii) access in the presence of school personnel; (iii) addition of a person to contact list; (iv) change of privacy settings.

What's allowed: search or compel student to produce data in the course of an investigation of policy violation or imminent threat to life or safety where there is reasonable suspicion that social media or device contains evidence. Monitoring use on institution's network and prohibiting use during school hours is permitted. Institution may monitor use of accounts created or provided by institution if the student is notified of such monitoring at the time the account is created.

What's the remedy: unclear. The statute itself provides none. No enforcement or remedies provisions are readily ascertainable.

Special notes: applies ONLY to educational institutions, not to employers. In cases of inadvertently receiving login, personnel must not access the account or device, not share the information with anyone, and delete it as soon as reasonably practicable.

7. Illinois

Statute: Codified at 820 ILL. COMP. STAT. 55/10 (2012) (employers); 105 ILL. COMP. STAT. 75/1-/20 (2013) (educational institutions) .

What's prohibited:

- **For employers:** the requested or required (i) turnover of account login; (ii) other employer access for employee and applicant accounts; (iii) access in employer's presence; and (iv) adding employer to contacts list. Retaliation for refusals and enforcement activities is also prohibited.
- **For educational institutions:** the requested or required turnover of account login or demand for access in any manner.

What's allowed: lawful workplace/school device and internet usage policies; network and e-mail monitoring without required login turnover; obtaining and using publicly available information regarding employees, applicants, or students; required cooperation during investigations.

What's the remedy: employee complaints to Dept. of Labor; Dept. investigations; employee private actions for actual damages, and for willful violations, actual damages, $200 penalty, plus attorneys' fees.

Special notes: e-mail is specifically excluded from "social networking website" definition; employer violations are also petty offenses with possible fines.

8. Louisiana

Statute: Codified at LA. REV. STAT. ANN. §§ 51:1951-:1955 (2014).

General overview: Governor Jindal signed the bill on May 22, 2014, and it went into effect on August 1, 2014.

What's prohibited: the requested or required (i) turnover of account login; and (ii) other employer access for employee and applicant personal accounts. This also applies to educational institutions' treatment of students or prospective students. Retaliation for refusals and enforcement activities is also prohibited.

What's allowed:

- **For employers:** access to an employer-provided account or device, discipline if an employee transfers proprietary information through a personal account, requiring employee to allow employer access in conjunction with an investigation for violations of state or federal law, or unauthorized transfer of proprietary information, but without requiring the employee to turn over login. An employer may also prohibit the use of certain websites while using an employer-owned device. Employer can utilize publicly available information found on social media sites.
- **For educational institutions:** access to a device or account supplied by the educational institution; viewing, accessing, or utilizing publicly available information online; restricting usage of certain websites while using a device owned or supplied by the educational institution.

What's the remedy: there is no remedy listed under this statute.

Special notes: no definition of "utilize" when describing how an employer/educator may use publicly available social media information, no remedy in the statute.

9. Maine

Statute: Codified at ME. STAT. tit. 26, §§ 616-619 (2015).

General overview: The bills were presented to Governor LePage on July 12, 2015, and became effective without his signature on October 15, 2015.

What's prohibited: the requested or required (i) turnover of account login; (ii) access in employer's presence; (iii) disclosure of account information; (iv) adding employer to contacts list; or (v) change of privacy settings.

What's allowed: required disclosure that employer reasonably believes to be relevant to an investigation or misconduct or law; accessing publicly available information; compliance with laws and regulations; and monitoring employer-issued accounts and devices.

What's the remedy: fines imposed by the Department of Labor of not less than $100 for the first violation, not less than $250 for the second violation, and not less than $500 for each subsequent violation.

Special notes: although educational institutions were included in the original bill, they are not included in the final bill except to the extent that the employer provisions apply to educational institutions.

10. Maryland

Statutes: Codified at MD. CODE ANN., LAB. & EMPL. § 3-712 (LexisNexis 2013) and MD. CODE ANN., EDUC. § 26-401 (LexisNexis 2015).

General overview: Governor O'Malley signed the employment-related bill on May 2, 2012, and it went into effect on October 1, 2012; Governor Hogan signed the education-related bill on May 12, 2015, and it went into effect on June 1, 2015.

What's prohibited:

- **For employers:** the requested or required (i) turnover of account login; and (ii) other employer access for employee and applicant personal accounts. Retaliation against employee or rejection of applicant for refusal is also prohibited. Also prohibits employees from downloading employer proprietary information or financial data without authorization.
- **For Post-Secondary Educational Institutions:** the requested or required (i) turnover of account login; (ii) access to accounts; (iii) adding certain contacts; or (iv) changing privacy settings for student and applicant personal accounts.

What's allowed: required turnover of non-personal account login; information-based investigations of (i) employee use of accounts for business purposes, for ensuring compliance; and (ii) prohibited employee information download.

What's the remedy: complaints to Labor Commissioner, who attempts informal mediation, or requests the attorney general to bring an action for damages, injunctions, "or other relief" on employee or applicant's behalf. A violated student may recover civil damages of up to $1,000.

Special notes: no specific damages are listed under the employer-related bill. No prohibition on retaliation for enforcement activities. Remedies section was added to employer-related law effective July 1, 2013.

11. Michigan

Statute: Codified at MICH. COMP. LAWS SERV. §§ 37.271-.278 (2012).

General overview: Governor Snyder signed the bill on December 27, 2012, and it became effective immediately.

What's prohibited: for employees, students, and applicants, the requested or required (i) disclosure of account content or "access information;" and (ii) observation of content. Disciplining employees or students, and rejection of applicants for refusals, is also prohibited.

What's allowed: mandatory employer access to its own device, or an account "provided by" the employer, obtained by virtue of the employment relationship, or "used for the employer's business purposes"; disciplining employees for transferring confidential information to a personal account without authorization; information-based investigations of account activity raising compliance or work-related misconduct issues, or unauthorized proprietary asset transfers; website restrictions and network monitoring in accordance with state and federal law; applicant screening and monitoring for self-regulatory companies; accessing and using publicly available employee and applicant information.

What's the remedy: criminal misdemeanor liability; employee, student, or applicant civil actions up to $1,000 plus attorneys' fees; mandatory pre-suit demand on violator for up to $1,000.

Special notes: "personal internet accounts" are not defined in terms of the purpose for the account, but only in technical terms. Nevertheless, the permitted employee access to accounts "provided by" the employer effectively defines personal accounts. Employers and educational institutions have immunity for "failing" to request or require employee, student, or applicant account access. The statute creates no duty for employers or educational institutions to search for or monitor accounts. It is an affirmative defense that the employer or educational institution "acted to comply" with federal or Michigan law.

12. Montana

Statute: Codified at MONT. CODE ANN. § 39-2-307 (2015).

General overview: Governor Bullock signed the bill on April 23,2015, and it became effective immediately.

What's prohibited: the requested or required (i) turnover of login information; (ii) access of employee personal accounts; (iii) divulgence of personal social media information for any personal accounts. An employer may not retaliate against an employee or applicant for refusing to comply with a request for this information.

What's allowed: an employer can request the personal login information if the employer has specific information about: (i) work-related misconduct; (ii) an unauthorized transfer of proprietary information or trade secrets; or (iii) when the employer is required to ensure compliance with

federal or state laws. Further, an employer can govern the use of employer-owned equipment or accounts, and may request the login information for those.

What's the remedy: civil liability in small claims court limited to $500 in actual damages plus legal costs to the prevailing party.

Special notes: there is nothing related to educational institutions in this bill. The remedies provide for fee-shifting for either prevailing party.

13. Nebraska

Statute: Codified at NEB. REV. STAT. ANN. §§ 48-3501--3511.

General overview: Governor Ricketts signed the bill on April 19, 2016, and it became effective July 21, 2016.

What's prohibited: the requested or required (i) turnover of account login; or (ii) access in employer's presence. Employer may not require an employee or applicant (i) to add anyone to a contacts list; or (ii) change privacy settings. Employee may not download or transfer proprietary information.

What's allowed: lawful policies governing employee use of employer equipment, disclosure of employee passwords to employer accounts and devices, monitoring and restricting employee use of employer networks and devices, accessing publicly available information, compliance with workplace and law enforcement investigations, and compliance with applicable laws and regulations.

What's the remedy: civil action within one year after the violation or discovery thereof. Successful complainants are entitled to appropriate relief, damages, reasonable attorney's fees and costs.

Special notes: Waivers or limitations of these protections as a condition of employment are unenforceable. There is an exception to this law for law enforcement agencies. In case of inadvertent discovery of login, employer shall not use the information or share it with anyone and shall delete it immediately.

14. Nevada

Statute: Codified at NEV. REV. STAT. § 613.135 (2013).

General overview: Governor Sandoval signed the bill on June 13, 2013, and it went into effect on October 1, 2013.

What's prohibited: requested or required turnover of employee or applicant personal account login or other information that provides account access; retaliation against employee or rejection of applicant for refusal is also prohibited.

What's allowed: required turnover of login for "other than personal" accounts in order to access employer's internal systems; applicant screening and monitoring for self-regulatory companies.

What's the remedy: unclear. Possible employee complaints with Nevada Human Rights Commission, in which remedies are limited to cease-and-desist orders, reinstatement and back pay, and benefits.

Special notes: no definition of "personal" or "other than personal" accounts; no exception for employer investigations of misconduct or information theft.

15. New Hampshire

Statute: Codified at N.H. REV. STAT. ANN. §§ 275.:73-:75. (2014) (employers); N.H. REV. STAT. ANN. § 189:70 (2015) (educational institutions).

General overview: Governor Hassan signed the employment-related bill on August 1, 2014, effective September 30, 2014. The education-related bill became law without Governor Hassan's signature on July 21, 2015, effective September 19, 2015.

What's prohibited:

- **For employers:** requiring or requesting an employee or applicant to (i) turnover login information; (ii) add a contact; or (iii) reduce privacy settings of a personal account. Further, an employer cannot take or threaten to take disciplinary action if an employee refuses to comply with an employer request for this information.
- **For educational institutions:** requiring or requesting a student or prospective student to (i) turnover login information; (ii) access an account in the presence of any institution employee; or (iii) change the privacy settings. Educational institutions also may not compel a student or prospective student to add anyone to a contacts list.

What's allowed:

- **For employers:** an employer may limit and monitor the use of employer-provided electronic equipment and may request login information for employer-provided

accounts. Further, an employer may view information that is publicly available. An employer may also conduct investigations into work-related misconduct based on information on an employee's personal account, or of allegations of unauthorized transfers of proprietary information. During such an investigation, the employer may ask the employee to share the content that has already been received to make factual determinations.

- **For educational institutions:** conducting investigations without requesting account login, revoking access to equipment or networks owned by the institution, monitoring usage on the institution's network, and requesting a student voluntarily share a printed copy of a specific communication from the student's account that is relevant to an investigation.

What's the remedy: civil penalties imposed by the Labor Commissioner after one written warning.

Special notes: even if the employer inadvertently acquires an employee's personal login information, it may not use it to access the employee's accounts. Also, the penalty scheme is quite sparse.

16. New Jersey

Statute: Codified at N.J. STAT. ANN. §§ 34:6B-5-10. (2014) (employers); N.J. STAT. ANN. § 18A:3-30 (2012) (educational institutions).

General overview: Governor Christie signed the employment-related bill on August 29, 2013, effective December 1, 2013. Governor Christie signed the education-related bill on December 3, 2012, effective immediately.

What's prohibited:

- **For employers:** for employees and applicants, the requested or required (i) turnover of personal account login or access information; and (ii) waiver of protected privacy rights; employee or applicant waiver is void as against public policy. Retaliation against employee or rejection of applicant for refusals is also prohibited.

- **For educational institutions:** to require a student or applicant to turnover login information or provide account access or to inquire as to whether a student or applicant has an account or profile on a social media site. Retaliation is also prohibited.

What's allowed: compliance with state and federal law, rules, regulations, case law, and self-regulatory screening requirements. Usage policies for employer devices, or accounts provided by the employer or used for employer business. Information-based investigations of account activity raising issues of work-related misconduct or employer-information theft. Obtaining and using publicly available information of employees and applicants.

What's the remedy: summary proceedings before the Labor Commission; maximum civil penalties of $1,000 for first violation; $2,500 for each subsequent violation. Governor Christie conditionally vetoed the civil-action section, which provided for injunctions, compensatory and punitive damages, attorneys' fees, and court costs. The legislature passed the more limited bill as conditionally vetoed without those remedies.

Special notes: defines "personal internet account" as an account (i) used exclusively for personal communications "unrelated to any business purpose of the employer"; and (ii) not an account "created, maintained, used, or accessed by an employee or accessed by an employee or applicant for business related communications or for a business purpose of the employer."

17. New Mexico

Statute: Codified at N.M. STAT. ANN. § 50-4-34 (2013) (employers); N.M. STAT. ANN. § 21-1-46 (2013) (educational institutions).

General overview: Governor Martinez signed the bill on April 5, 2013, and it became effective immediately.

What's prohibited: for applicants and students only (not for employees), the requested or required (i) turnover of account login; and (ii) other account access. Rejection of applicant for refusal is also prohibited.

What's allowed: lawful workplace policies regarding device and network usage; equipment and network monitoring without mandatory account access; obtaining and using publicly available applicant information.

What's the remedy: unclear. New Mexico has an Employee Privacy Act (N.M. STAT. ANN. §§ 50-11-1 to -6 (1991)) which prohibits employer discrimination against smokers, and allows civil actions, damages, and attorneys' fees, but it is unknown whether the new social networking law will be incorporated into that Act or some other statutory framework.

Special notes: the prohibitions are not limited to applicants' personal accounts though because they do not yet have any employer-provided accounts; perhaps the personal account limitation is implied. No exception for employer investigations of misconduct or information theft.

18. Oklahoma

Statute: Codified at OKLA. STAT. tit. 40 § 173.2 (2014).

General overview: Governor Fallin signed the bill on May 21, 2014, and it became effective November 1, 2014.

What's prohibited: requiring an employee or prospective employee to (i) turnover login information; or (ii) access an account in the employer's presence. Retaliatory action against an employee or prospective employee for refusing to comply with such a request is prohibited.

What's allowed: employers may conduct investigations into (i) work-related misconduct based on information found on an employee's personal account; or (ii) unauthorized transfers of proprietary information. An employer may require the employee's cooperation to share the content that has been reported to make factual determinations. An employer may view and monitor personal content that an employee chooses to access on an employer-owned device.

What's the remedy: civil action may be brought within six months of the alleged occurrence, and the employee may receive $500 in damages per violation.

Special notes: the statute specifically forecloses the possibility of punitive or emotional damages.

19. Oregon

Statutes: Codified at OR. REV. STAT. § 659A.330 (2015) (employers); OR. REV. STAT. §§ 350.272-.274 (2015) (educational institutions).

General overview: Governor Kitzhaber signed the employer-related bill on May 22, 2013, effective January 1, 2014. An amendment to the statute was enacted on June 2, 2015, and it became effective on January 1, 2016. Governor Kitzhaber signed the education-related bill on June 13, 2013, effective January 1, 2014. The statute was renumbered in 2015.

What's prohibited:

- **For employers:** for employees and applicants, the requested or required turnover of personal account login. Employers are also prohibited from requiring an employee or applicant (i) to allow an employer to advertise on his or her personal social media account; (ii) to add an employer to a contacts list; or (iii) to access an account in an employer's presence. Retaliation against existing employees and rejection of applicants for refusal is prohibited.
- **For educational institutions:** the requested or required (i) turnover of personal account login; or (ii) accessing an account in an employer's presence. Educational institutions may not take or threaten to take any disciplinary action against a student, or refuse to admit a prospective student, as a result of his or her refusal to disclose social media account information.

What's allowed: mandatory access to non-personal accounts to provide access to employers' internal computer, IT systems; viewing publicly available information; accessing information, without requiring an employee to provide a user name and password, to conduct an investigation.

What's the remedy: employees and job applicants, or the attorney general, may sue for a minimum $200 penalty punitive damages, injunctions, attorneys' fees, reinstatement, back pay, and "other appropriate relief." Students and applicants must first exhaust certain administrative remedies with the school's administration.

Special notes: In the amended statute, definitions of "personal social media account" and "social media" have been added. The student / school applicant administrative remedies requirements are unique.

20. Rhode Island

Statutes: Codified at R.I. GEN. LAWS §§ 28-56-1 to -6 (2014) (employers); R.I. GEN. LAWS §§ 16-103-1- to -6. (2014) (educational institutions).

General overview: Governor Raimondo signed the bills on June 30, 2014, and the bills became effective upon passage.

What's prohibited: requiring, requesting, or coercing an employee, student, or applicant to (i) turnover login information; (ii) access an account in an employer's or representative's presence; (iii) divulge information; (iv) add contacts; or (v) change privacy settings to personal social media accounts. Retaliation against anyone for refusing to comply with any of the aforementioned requests is prohibited.

What's allowed: employers may require an employee to divulge personal social media account information in conjunction with an investigation into workplace-related misconduct or violations of federal or state law. Employers and educational institutions may access publicly available information.

What's the remedy: civil damages, injunctive relief, reasonable attorneys' fees and costs.

Special notes: there is no statutory cap or parameter for damages.

21. Tennessee

Statute: Codified at TENN. CODE ANN. §§ 50-1-1001 to -1004. (2014).

General overview: Governor Haslam signed the bill on May 16, 2014, and it became effective on January 1, 2015.

What's prohibited: requiring or requesting an employee or applicant to (i) turnover a password; (ii) add an employer to a list of contacts; or (iii) allow employer access to a personal internet account. Retaliation for refusal to comply with such a request is prohibited.

What's allowed: requiring an employee to disclose a user name and password for (i) an employer-provided account or device; or (ii) in conjunction with an investigation of work-related misconduct or an unauthorized transfer of proprietary information. An employer may also restrict or monitor access to certain web sites while on an employer-owned network or device. Furthermore, an employer may view and use information about an employee that is publicly available.

What's the remedy: civil action with damages of not more than $1,000 per violation plus reasonable attorneys' fees and court costs.

22. Utah

Statutes: Codified at UTAH CODE ANN. §§ 34-48-101 to -301. (LexisNexis 2013) (employers); UTAH CODE ANN. §§ 53B-25-101 to -301 (LexisNexis 2013) (educational institutions).

General overview: Governor Herbert signed the bills on March 26, 2013, and they went into effect on May 14, 2013.

What's prohibited: for employees, applicants, students, and prospective students, requested or required turnover of personal account login. Retaliation against existing employees or rejection of applicants for refusal is also prohibited.

What's allowed: mandatory login turnover to access (i) employer or institution device; or (ii) employer- or institution-provided account used for employer business or educational purposes, disciplining employees for employer information theft, information-based investigations (including requiring employee cooperation in investigations, of (i) employee account activities which raise compliance issues; or (ii) employer information theft), restricted access on employer's network and devices, accessing and using publicly available employee, applicant, student, and prospective student information.

What's the remedy: civil action with a maximum award of $500.

Special notes: defines "personal internet account" as an account (i) used exclusively for personal communications "unrelated to any business purpose of the employer;" and (ii) not an account "created, maintained, used, or accessed by an employee or accessed by an employee or applicant for business related communications or for a business purpose of the employer." Statute does not create employer duty to monitor employee personal account activity. Contains employer immunity for not requesting or requiring employee's or applicant's personal account login or access.

23. Vermont

Statute: H.B 462, 2017 Leg., 74th Sess. (Vt. 2017) (not yet codified).

General overview: Governor Scott signed the bill on May 17, 2017, and it goes into effect January 1, 2018.

What's prohibited: for applicants and employees, the required or requested (i) turnover of employee personal account login; (ii) access of account in employer's presence; (iii) divulging of social media content to employer; or (iv) change of privacy settings. An employer may not require an employee or applicant to add anyone to a contacts list. Retaliation against an employee who exercises these rights is prohibited.

What's allowed: compliance with legal and regulatory obligations; investigating alleged unauthorized transfer or disclosure of proprietary information, unlawful harassment, threats of violence, or discrimination. Law enforcement agencies are permitted to request or require access for screening or fitness determinations and investigations. Employers may request or require turnover of login information for an employer-issued device

What's the remedy: None mentioned.

Special notes: any agreement by an employee to waive his or her rights is invalid.

24. Virginia

Statute: Codified at VA. CODE ANN. § 40.1-28.7:5 (2015) (employers); VA. CODE ANN. § 23.1-405 (2016) (educational institutions).

General overview: Governor McAuliffe signed the employment-related bill on March 23, 2015, effective July 1, 2015. Governor McAuliffe signed the education-related bill on April 1, 2016, effective October 1, 2016.

What's prohibited:

- **For employers:** requiring an employee or prospective employee to (i) turnover login information; or (ii) add an employer to a list of contacts for personal social media accounts. An employer may not use inadvertently received login information to gain access to the employee or prospective employee's account. Retaliation for refusal to comply with an aforementioned request is prohibited.

- **For educational institutions:** requiring a student to turnover login information.

What's allowed: viewing publicly available information about a current or prospective employee, requesting an employee to disclose login information in conjunction with a formal investigation of employee misconduct or violation of federal or state laws. Campus police officers are not prevented from performing official duties.

What's the remedy: no remedies are listed in the statute.

Special notes: the statute does not list any remedies; the statute only prohibits the employer "requiring" the turnover of login information, but does not specifically say anything about the "request" being prohibited.

25. Washington

Statute: Codified at WASH. REV. CODE §§ 49.44.200-.205 (2013).

General overview: Governor Inslee signed the bill on May 21, 2013, effective July 28, 2013.

What's prohibited: requiring or requesting an employee or applicant to (i) turnover personal account login; (ii) allow employer observation of account content; (iii) add employer to contacts list; and (iv) make privacy-settings changes. Retaliation against employee or rejection of applicant for refusal is also prohibited.

What's allowed: mandatory access to personal account (but not mandatory login turnover) for information-based investigation of personal account activity raising issues of compliance, work-related misconduct, or information theft. Mandatory access to employer-provided accounts and employer-owned devices. Enforcement of personnel policies consistent with the statute, and any other state or federal requirements under statute, regulations, or case law trump the privacy statute.

What's the remedy: employees and job applicants may sue for actual damages, $500 penalty, injunctions, attorneys' fees, reinstatement, back pay, and "other appropriate relief."

Special notes: the permitted mandatory account access, but not mandatory account login turnover, is unique. The statute does not define personal accounts. Contains "innocent discovery" rule which protects employers that inadvertently learn protected login information, so long as the employers do not use it to access personal accounts. Contains an attorney-fee shift provision against employee plaintiffs for frivolous actions "without reasonable cause."

26. West Virginia

Statute: Codified at W. VA. CODE § 21-5H-1 (2016).

General overview: Governor Tomblin signed the bill on April 1, 2016, effective June 10. 2016.

What's prohibited: the required or requested (i) turnover of account login; or (ii) access in the presence of the employer. Employers may not compel employees or potential employees to add the employer to a contacts list that enables access to a personal account

What's allowed: accessing publicly available information, compliance with applicable laws, accessing employer-issued devices and accounts, requiring an employees to share content during investigations

What's the remedy: unclear. No remedies are mentioned in the statute.

Special notes: In cases of inadvertent receipt of login information, an employer is not liable for having the information unless the employer (i) uses the information to access the account; (ii) enables a third party to use the information to access the account; or (iii) does not delete the information as soon as reasonably practicable after it is discovered.

27. Wisconsin

Statute: Codified at WIS. STAT. § 995.55 (2014).

General overview: the legislature passed 2013 Senate Bill 223 on February 10, 2014. Governor Walker signed the bill on April 8th and the law went into effect on April 10, 2014.

What's prohibited: for current or prospective employees, students, and tenants, the requested or required turnover of personal account access information, or other required account access or observation. Retaliation against current or prospective employee, student, or tenant for refusal is also prohibited.

What's allowed: mandatory access to employer-provided accounts, non-personal accounts, and employer-owned and school-owned devices. Adverse employment action for proprietary-information or financial data theft. Mandatory access to personal account (but not mandatory login turnover) for information-based investigation of personal account activity raising issues of compliance, work-related misconduct, or information theft. Compliance with pre-employment screening required by law. Accessing and using employee, student, and tenant information available in the public domain. Internet-site restrictions using employer-owned devices or networks. Mandatory disclosure of employee personal email addresses.

What's the remedy: maximum $1,000 forfeiture. Current or prospective employees and students may file complaints with department of workforce development. After finding probable cause of a violation and subsequent hearing, the department may order appropriate remedial relief, including back pay, reinstatement, or front pay under certain limits.

Special notes: "personal" accounts are those which are used exclusively for personal purposes. Specifies that no employer, school, or landlord has a duty to search or monitor personal account activity, and that none of them are liable for failing to demand account access when arguably authorized to do so. Contains "innocent discovery" rule which protects employers and schools that inadvertently learn protected login information, so long as the employers do not use it to access personal accounts. Union employees whose collective bargaining agreements conflict with the Act are protected upon the expiration of the CBA which exists as of the Act's effective date, or when that CBA is renewed or extended.

WHAT DOES THE TERM "PERSONAL" TRULY MEAN IN SOCIAL MEDIA LEGISLATION?

Many states, including California, Colorado, Nevada, and Washington, have passed social media privacy laws that do not define the term "personal." Although the state laws discussed here generally apply only to "personal" social media accounts, the failure to define the term is problematic, as it can be unclear who owns particular social media accounts in the absence of clear policies and agreements.

Based on the courts' decisions over the last few years, employers likely have at least some ownership rights to an employee's social media account (even if the account is used for both company and personal purposes) if the employer plays an important role in creating, maintaining or developing the account. See, e.g., *Cellular Accessories For Less, Inc. v. Trinitas LLC,* No. CV 12-06736, 2014 WL 4627090 (C.D. Cal. Sept. 16, 2014) (employer may have an interest in contacts in employee's LinkedIn account); *Eagle v. Morgan,* No. 11-4303, 2011 WL 6739448 (E.D. Pa. Dec. 22, 2011) (same); *PhoneDog v. Kravitz,* No. C11-03474 MEJ, 2011 U.S. Dist. LEXIS 129229 (N.D. Cal. Nov. 8, 2011) (former employer may have interest in employee's Twitter account).

Employers could potentially evade the new privacy laws by including phrases in employee job descriptions detailing their ownership of these work accounts. By including requirements that an employee use such accounts in job descriptions and in proprietary information protection agreements, an employer can attempt to ensure that company social media accounts belong to the company, even after the employee departs.

BRING YOUR OWN DEVICE POLICIES

Employers may also face additional issues resulting from bring your own device ("BYOD") policies. When an employee uses his or her own personal device to access company email, files, or other information, the employer may not own the device, but still has an interest in the information residing on the device. Although the employer may not technically own the device, the company still has an interest in protecting its data and information. As such, state legislatures would be wise to clarify the definition of "personal" to ensure that the enforcement of state laws does not have unintended consequences, including employees blocking access to company files on personal devices based on privacy. Furthermore, public employers have a heightened interest restricting employees' use of personal mobile devices to conduct official business. See *Nissen v. Pierce Cty.,* 183 Wash. 2d 863, 869 (Wash. 2015) (en banc) (holding text messages sent and received by a public employee in her official capacity were public records even though she was using her personal cell phone).

An effectively written BYOD policy can protect an employer's interest in the data. A policy that clearly informs employees that all company-related information on the device remains the sole property of the company and that the company retains the right to delete company data through the use of monitoring software can establish the company's control over the information. See *H.J. Heinz Co. v. Starr Surplus Lines Ins. Co.,* Civil Action No. 2:15-cv-00631-AJS, 2015 WL 12791338 (W.D. Pa. July 28, 2015) (plaintiff maintained custody and control of data pursuant to company policy).

TRADE SECRETS

As touched on above, social media privacy laws may conflict with recent decisions about whether social media account content, including contact lists, may be employers' protectable trade secrets. Where is the line between personal and business relationships? Social media privacy laws also raise questions on whether employers waive trade secret protection for social media account information or fail to properly safeguard it if they could have required access to accounts of employees who steal company data, but did not do so. Accordingly, to minimize these new privacy laws' impact on their intellectual property assets, it is a good idea for employers to audit their IP-protection policies and procedures and ensure that they have written social media policies/agreements specifying ownership of the account and connections within the account.

A. Definition of a Trade Secret - Brief Summary.

In the simplest terms, under the Uniform Trade Secrets Act ("UTSA"), which is in effect in 48 states, information and data may qualify for statutory protection if the valuable information is a secret, and its owner keeps it a secret. In the two states that have not yet adopted the UTSA (New York and Massachusetts), common law provides similar protections for trade secrets. Though there are no bright lines for whether information is a protectable trade secret, courts generally find that information is protectable as a trade secret if (i) the information is the result of a substantial investment of time, effort, and expense; (ii) it generates independent economic value for its owner; (iii) it is not generally known in the relevant industry; (iv) it cannot easily be accessed by legitimate means, and (v) it cannot be independently reverse engineered without significant development efforts and expense. Experience shows that in many cases, the more egregious a defendant's theft of an alleged secret, the more likely the court will find that the stolen data qualifies as a trade secret. This is the case

not merely because of the court's understandable desire to punish egregious behavior but because an employee's theft and subsequent use of stolen data or information tends to show the independent economic value of the stolen information and also tends to show that the information was not available publicly.

Information is kept secret if its owner takes affirmative measures to prevent its unauthorized disclosure, such as (but not limited to) non-disclosure, restricted-use, and mandatory-return agreements, confidentiality stamps, limited internal distribution and access permissions, and password protection of computers. Those efforts need only be "reasonable under the circumstances," and "absolute" secrecy is not required.

B. Social Media Privacy Laws' Potential Impact on Account-Content Ownership.

Social media privacy laws may be relevant to trade-secret-ownership lawsuits between companies and their former employees regarding who owns the latter's social media contact information (i.e. LinkedIn contacts). The cases cited above, *PhoneDog, Eagle,* and *Cellular Accessories,* held that the company's Twitter feeds (PhoneDog) and the employee's LinkedIn account (*Eagle* and *Cellular Accessories*) may "belong to" the employer, due to the employer's prior investment of time and expense in developing and maintaining those accounts. Further, in *Ardis Health, LLC v. Nankivell,* No. 11 Civ. 5013(NRB), 2011 WL 4965172 (S.D.N.Y. Oct. 19, 2011), the court held that the employer owned its employee's account content, due to the wording in the employment agreement. More recently, in *Salonclick LLC v. SuperEgo Mgmt. LLC,* 16 Civ. 2555 (KMW), 2017 WL 239379 (S.D.N.Y. Jan. 18, 2017), the court extended companies' rights to protect their social media accounts and domain names from theft by independent contractors.

However, with the onset of social media privacy laws, will employees have ammunition to argue that they own their social-media contacts, especially in states where personal and non-personal accounts are not clearly defined? Employees in trade secrets cases may argue that social media privacy laws imply a degree of ownership of their social media accounts, even where they use them in part to advertise their employers' businesses.

C. Social Media Privacy Laws' Impact on the Protective-Measure Analysis in Trade Secrets Cases.

Further, some might argue that, unless employers investigate their employees' social media activities and any related data theft, employers will lose trade secret protection for that data due to their alleged failure to use "reasonable" efforts to protect its secrecy. Under the Uniform Trade Secrets Act section 1(4)(ii), trade secret owners must have employed "efforts that are reasonable under the circumstances to maintain its secrecy." The "reasonable under the circumstances" requirement is often the key disputed issue in trade secrets litigation — the owner claiming that it used reasonable efforts; the alleged thief claiming that the plaintiff was too "willy-nilly" in handling its so-called secrets. If social media privacy laws permit an employer to investigate an employee's suspected data theft through his social networking account, but the employer does not do so, has the employer failed to use "reasonable efforts" to protect the data's secrecy?

On the one hand, information that falls into the public domain, or becomes generally known to the relevant industry, usually loses its trade secret status. See, e.g., *Newark Morning Ledger Co. v. New Jersey Sports & Exposition Authority,* 31 A.3d 623, 641 (N.J. App. 2011) (trade secrets' "only value consists in their being kept private . . . if they are disclosed or revealed, they are destroyed"). Similarly, information that its owner discloses without imposing a confidentiality obligation on the recipient is at high risk of losing any secrecy protection. See *Seng-Tiong Ho v. Taflove,* 648 F.3d 489, 504 (7th Cir. 2011) (plaintiff's publishing its alleged secrets in trade journals destroyed any trade secret status that information had). An employee's posting of confidential employer data on his or her social networking account would pose a significant risk that the data would lose its trade secret protection, especially if the employer was authorized by the applicable privacy law to demand access to the employee's account to investigate, but for whatever reason did not or had policies that did not prohibit such social media activities.

On the other hand, "absolute" secrecy is not required to maintain trade secrecy, but only reasonable efforts to maintain confidentiality. See, e.g., *Avidair Helicopter Supply, Inc. v. Rolls-Royce Corp.,* 663 F.3d 966, 974 (8th Cir. 2011) (efforts to maintain secrecy "need not be overly extravagant, and absolute secrecy is not required"). Indeed, two relevant features of many privacy laws are (i) employer immunity for not investigating suspected misconduct (see Michigan and Utah); and (ii) no duty to monitor employee account activity. Employers faced with a waiver argument may cite these statutory provisions to counter the argument that they were required to investigate reports of employee-account-related data theft, lest they lose statutory protection for that data.

SOCIAL MEDIA DISCOVERY ISSUES

Under the Federal Rules of Civil Procedure, parties may request discovery of "electronically stored information" that is within the responding party's "possession, custody, or control." Fed. R. Civ. P. 34(a)(1)(A). Courts have recognized that information available on social networking websites may be subject to discovery under this rule. See *Davenport v. State Farm Mut. Auto. Ins. Co.,* 3:11–CV–632–J–JBT, 2012 WL 555759, at *1 (M.D. Fla. Feb. 21, 2012); *Mailhoit v. Home Depot U.S.A., Inc.,* 285 F.R.D. 566, 570 (C.D. Cal. 2012). According to the U.S. District Court of Oregon, there is "no principled reason to articulate different standards for the discoverability of communications through email, text message, or social media platforms." *Robinson v. Jones Lang La Salle Americas, Inc.,* No. 3:12-CV-00127, 2012 WL 3763545, at *1 (D. Or. Aug. 29, 2012).

Generally, social media is neither privileged nor protected by any right of privacy. *Davenport,* 2012 WL 555759 at *1; *Tompkins v. Detroit Metro. Airport,* 278 F.R.D. 387, 388 (E.D. Mich 2012). According to one federal court, content from social networking websites isn't "shielded from discovery simply because it is 'locked' or 'private.' Although privacy concerns may be germane to the question of whether requested discovery is burdensome or oppressive and whether it has been sought for a proper purpose in the litigation, a person's expectation and intent that her communications be maintained as private is not a legitimate basis for shielding those communications from discovery." *EEOC v. Simply Storage Mgmt., LLC,* 270 F.R.D. 430, 434 (S.D. Ind. 2010). A party's right to discovery is not unlimited, however, and "may be curtailed when it becomes an unreasonable annoyance and tends to harass and overburden the other party." *Fawcett v. Altieri,* 960 N.Y.S. 2d 592, 594 (2013). Fed. R. Civ. P. 26(b)(1) limits discovery to information "that is relevant to any party's claim or defense and proportional to the needs of the case." This rule is applicable to social media. See *Gordon v. T.G.R. Logistics, Inc.,* Case No. 16-CV-00238-NDF, 2017 WL 1947537, at *3-4 (D. Wyo. May 10, 2017) (limiting discovery of social media to posts related to contested issues rather than the entire account history).

Recent case law on social media discovery has focused on the importance of maintaining such information and preventing spoliation. In fact, social media and privacy issues are a growing headache for many general counsel, with more companies having to preserve data from employees' social media accounts. In *Gatto v. United Air Lines,* Civil Action No. 10-cv-1090-ES-SCM, 2013 WL 1285285 (D.N.J. Mar. 25, 2013), the plaintiff sued his employer based on injuries suffered while working. During discovery, the defendants requested the plaintiff's social networking account content, and the plaintiff agreed to provide account access. Upon opposing counsel's initial login, however, the plaintiff received notice of unauthorized access and immediately deactivated his account. The court granted spoliation sanctions against the plaintiff. The court found that regardless of whether he intended to destroy the account, the plaintiff "effectively caused the account to be permanently deleted," which rendered a spoliation inference appropriate. *Id.* at *4.

In a similar case, *Lester v. Allied Concrete Co.,* No. CL08-150, 2011 Va. Cir. LEXIS 245 (Va. Cir. Ct. Sept. 6, 2011), a Virginia court sanctioned a party and his lawyers in a wrongful death suit for intentionally destroying a Facebook page. In that case, the opposing party requested discovery of the contents of the plaintiff's Facebook page after it obtained a photo of the plaintiff wearing an "I [heart] hot moms" T-shirt. *Id.* at *12. After the plaintiff had been questioned about the shirt at his deposition, his attorney instructed him to "clean up" the account to prevent "blowups of this stuff at trial." *Id.* at *13. The account was removed, and defense counsel was told that plaintiff had no Facebook page. *Id.* at *15. The account was later reactivated and the contents were produced, with the exception of a number of objectionable photos. *Id.* at *17. Although the jury found in favor of plaintiff, the court sanctioned plaintiff and his attorney for spoliation as a result of the deletion of the page. *Id.* at *40.

In summary, the new privacy laws may have some effect on whether protected account content is discoverable in litigation, but probably not much. The new legislation may be cited as support in opposition to discovery of protected content, but courts will still likely order disclosure, perhaps subject to heightened protective orders.

SOCIAL MEDIA EVIDENCE REQUIREMENTS

For social media evidence to be admissible, the proponent must be able to prove who had ownership and control of the page. Fed. R. Evid. 901 requires the proponent to produce evidence proving an item is what the proponent claims it is. Social media is not exempt from this rule. See *United States v. Vayner,* 769 F.3d 125, 132 (2d Cir. 2014) (holding that evidence of the existence of a social media page containing defendant's name and photograph was not enough to prove it belonged to the defendant unless the government could prove that the defendant had created the page or was responsible for its contents). Arguments that social media pages are self-authenticating will likely fail. See *United States v. Browne,* 834 F.3d 410-11 (3d Cir. 2016)

(holding that social media posts are not self-authenticating under the business records exception because records custodians can only attest to communications taking place between accounts, not who authored the posts, and there is no underlying process by which the information is recorded that would render the posts accurate and trustworthy).

Additionally, evidence procured from a social media account is subject to Fed. R. Evid. 403, which requires a balancing test to determine whether the probative value of evidence is substantially outweighed by danger of unfair prejudice. Rule 403 applies even when a proponent is introducing evidence to authenticate a social media page, but the bar for admissibility is relatively low. See *State v. Ford,* 782 S.E.2d 98, 106-07 (N.C. Ct. App. 2016) (admitting screen shots of defendant's allegedly vicious dog and a rap video from his MySpace page to prove the page belonged to defendant, despite his objections that the content prejudiced the jury to believe that his dog had, in fact, killed the victim). Although "tracking the webpage directly to [its purported creator] through an appropriate electronic footprint or link would provide some technological evidence, such evidence is not required . . . where strong circumstantial evidence exists that [a] webpage and its unique content belong to [such person]." *Id.* at 106.

The rulings in *Vayner, Browne,* and *Ford* indicate that traditional rules of evidence are applied with a common sense approach to social media-related issues. Authentication of records is critical for proponents attempting to introduce social media posts.

COMPUTER FRAUD AND ABUSE ACT AND PRIVACY IMPLICATIONS

The new privacy legislation may affect how courts decide employees' allegations against their employers for violations of the federal Computer Fraud and Abuse Act ("CFAA") and the employees' common law rights of privacy.

One case that highlights these issues is *Mintz v. Mark Bartelstein & Assocs. d/b/a Priority Sports & Entm't et al.,* 885 F. Supp. 2d 987 (C.D. Cal. 2012), where the court found that accessing the personal email account of an employee, even one who had allegedly stolen trade secrets, was an invasion of the employee's privacy. *Id.* at 1002. There, an employee (Mintz) resigned from his job and sued his former employer after he left to join a competitor, seeking declaratory relief to invalidate his non-compete agreement. *Id.* at 989. After Mintz's resignation, his employers accessed Mintz's personal email account without his permission, and allegedly leaked information found in the account to a third party. *Id.* at 990. The court denied recovery under the CFAA, finding that Mintz had failed to show loss, as his legal fees were paid by his new employer. *Mintz v. Mark Bartelstein & Assocs.,* 906 F. Supp. 2d 1017, 1031 (C.D. Cal. 2012). Furthermore, the expenses of litigation were not a loss as they were not "essential to remedying the harm of the unauthorized access." *Id.* at 1030. However, the court did find that the employer's access to Mintz's Gmail account constituted a violation of California Penal Code section 502, as well as an invasion of privacy. *Id.* at 1032, 1035.

Similarly, in a case arising out of Oklahoma, a federal court held that an employer's access of an employee's personal email account to obtain information used in recommending her termination could be the basis for a claim of invasion of privacy. In *Murphy v. Spring,* No. 13-CV-96-TCK-PJC, 2013 U.S. Dist. LEXIS 130231, at *2 (N.D. Okla. Sept. 12, 2013), an administrative assistant working in a school district in Tulsa, Oklahoma acted as a whistleblower, alleging that two of her superiors had misappropriated funds, and endangered the health and safety of the students. Shortly after making these reports, the assistant was suspended, and her boss recommended she be terminated. *Id.* The assistant instigated the grievance process. *Id.* During this process, she was informed by the local police department that her private email account had been hacked. *Id.* at *3. She sued her employer, alleging that her employer had intentionally obtained access to her private emails, and had used this information in recommending her termination. *Id.* at *4–5. The court denied the employer's motion to dismiss her Fourth Amendment claim, privacy claim, and claim for intentional infliction of emotional distress, finding that the plaintiff had a reasonable expectation of privacy in her personal account, and the hacking constituted an unlawful search and seizure which could be considered highly offensive to a reasonable person. *Id.* at *34.

The rulings in *Mintz* and *Murphy* suggest that employers should use caution in accessing employees' personal email accounts, as there can be consequences for employers who do so. In addition to liability under state social media laws, employers may also be liable under state computer hacking laws or an invasion of privacy action. While the plaintiff in *Mintz* could not maintain a claim under the CFAA because to there was no "loss" and his subsequent legal efforts to confirm the employer's involvement were not "essential to remedying the harm" of the unauthorized access, he was able to maintain a California Penal Code section 502 claim, as well as an invasion of privacy claim, based upon the same conduct.

In addition, the new legislation, which in many respects demonstrates that unjustified employer access is prohibited, may bolster an employee's "without authorization" claim

under the CFAA. Before the new legislation, an employer's accessing the account without its employee's permission may not have been "unauthorized," assuming the employee used an employer's device. The bottom line: employers should proceed very cautiously before investigating their employees' personal email accounts or personal or social media accounts, even if conducting a workplace investigation, unless they receive express written consent from the employees in question.

USING SOCIAL MEDIA IN INVESTIGATIONS

When using social media posts in workplace investigations, employers should stay within the bounds of their own social media policies. Although viewing information from an employee's social media account that is available on the public domain is permitted (even in states that have social media privacy laws), employers should take care not to take actions that may be perceived as retaliation for protected activities.

For example, in *Jones v. Gulf Cost Health Care of Del., LLC,* 854 F.3d 1261, 1275 (11th Cir. 2017), an employer confronted an employee with vacation pictures he had posted on Facebook while he was on FMLA leave and subsequently terminated his employment for FMLA abuse and misuse. Later, however, the employer claimed that the reasons for termination were the employee's poor judgment in posting the pictures and the employee's violation of the employer's social media policy, which prohibited posts that could have a negative impact on coworkers. *Id.* at 1274-75. Reversing the lower court's dismissal of the plaintiff's FMLA retaliation claim, the 11th Circuit held that, due to the employer's inconsistent reasoning and its inability to point to any employees who were adversely affected by the plaintiff's posts, its proffered reasons for termination may have been pretext for discrimination. *Id.* at 1275.

Social media policies can create an extension of other workplace policies. A well-written social media policy can be an effective tool for employers to enforce prohibitions on employee behavior outside the workplace. See *Jackson v. Walgreen Co.,* 516 S.W.3d 391, 394-95 (Mo. Ct. App. 2017) (affirming Labor and Industrial Relations Commission's denial of unemployment benefits when employee was terminated for harassing coworkers online in violation of company's social media policy, which specifically prohibited such conduct). As with any workplace policy, it is important for employers to enforce social media policies consistently. See *Carney v. City of Dothan,* 158 F. Supp. 3d 1263, 1282, 1292-93 (M.D. Ala. 2016) (granting employer's motion for summary judgment in race discrimination case because employer was justified in taking adverse employment action against employee who violated its social media policy and employer could show that it consistently investigated potential violations regardless of employee's race).

Having an effectively written social media policy is the first step for an employer to protect itself during workplace investigations. Simply having a policy, however, is not enough. As demonstrated by *Jones, Jackson,* and *Carney,* managers must be properly trained on utilizing the policy appropriately and consistently for the employer to realize its full benefits.

OTHER ISSUES

In addition to complying with state social media privacy laws, employers should carefully consider whether their social media policies comply with federal and state laws protecting the ability of employees to engage in statutorily protected activities. From the Equal Employment Opportunity Commission ("EEOC") and the Department of Labor ("DOL") to the Securities and Exchange Commission ("SEC") and the National Labor Relations Board ("NLRB"), federal and state regulatory agencies are increasingly clamping down on employer policies that limit the ability of employees to engage in whistleblowing or other protected activities. Depending on how broadly their policies are worded, employers' social media policies potentially can run afoul of statutory provisions as interpreted by these agencies.

Of particular note, the NLRB is increasingly taking a hard look at employer policies on use of social media. In its 2014 decision in *Triple Play Sports Bar & Grille,* 361 NLRB No. 31 (2014), the NLRB ruled that a Facebook discussion regarding an employer's tax withholding calculations and an employee's "like" of the discussion constituted concerted activities protected by Section 7 of the National Labor Relations Act ("NLRA"), which protects employees' rights to engage in concerted activities regarding the terms and conditions of their employment. In addition, in the *Triple Play* decision, the Board held that the employer's internet and blogging policy (which provided that "engaging in inappropriate discussions about the company, management, and/or co-workers, the employee may be violating the law and is subject to disciplinary action, up to and including termination of employment") was overly broad and, therefore, violated the NLRA. Moreover, in another decision, *Purple Communications,* 361 NLRB No. 126 (2014), the NLRB ruled that employees who have access to an employer's email system as part of their job generally may, during non-working time, use the email system to communicate about wages, hours, working conditions and union issues. In light

of these rulings, employers should carefully consider their policies and practices regarding employee use of social media even if they operate only in states that have not yet enacted employee social media privacy laws.

TAKEAWAYS

Issues related to social media privacy in the workplace are not going away, and we expect to see more litigation and legislation to define acceptable practices in this area. In light of this uncertainty, employers should at a minimum do the following:

1. Determine whether your company has employees in any of the states that have adopted or are planning to adopt social media privacy laws.

2. Review existing policies and agreements regarding employees' use of social media and computer resources for business purposes to ensure that those policies and agreements clearly define ownership and access rights for such accounts.

3. Consider whether to block access to social networking sites not used for business purposes, as well as to other categories of potentially problematic Internet web sites that might be protected under some states' statutes, such as file-sharing and internet-mail sites.

4. Ensure that those involved in an investigation addressing an employee's social media activity are aware that state laws may restrict requests for information about such activity. Counsel should review the applicable state social media access law before asking an employee for any account-related information.

5. Provide recurring training on the company's social media policy, confidentiality policies, and agreements and remind employees that the same confidentiality policies and agreements that apply in the workplace also apply to their social media activities.

6. Evaluate the company's computer network to reduce the opportunities for incidents of employee misconduct and network security breaches.

7. Don't overlook social media evidence in conducting employee investigations and in employee lawsuits, including any necessary preservation obligations, but make sure that your company's review and access of such information does not violate applicable law.

8. Evaluate whether the benefits of a bring your own device policy outweighs the risks to data security confidentiality, and employee privacy.

9. Social media policies should be narrowly tailored and provide examples of protected confidential information so that they do not run afoul of NLRB guidelines.

CONCLUSION

As of November 2017, 27 states are considering or have already introduced social media legislation. States throughout the country are currently considering this relevant issue, and it is likely we will see additional states pass similar social media legislation before the year is out. To stay current on the latest developments in social media privacy, please follow our blog at www.tradesecretslaw.com.

State-by-State Chart

STATE	Are personal social media accounts covered by the law?	Is personal social media defined?	Is there a private civil right of action?	Are current employees covered by the law?	Are attorneys fees available?	Does the law cover colleges and universities?	Are public employees covered by the law?	Exceptions for investigations of employee misconduct?
Arkansas	Yes	Yes	Not Mentioned	Yes	Not Mentioned	Yes	Yes	Yes
California	Yes	No	Not Mentioned	Yes	Not Mentioned	Yes	Not Mentioned	Yes
Colorado	Yes	No	Yes	Yes	Not Mentioned	Not Mentioned	Yes Law Enforcement Agencies Exception	Not Mentioned
Connecticut	Yes	Yes	Yes	Yes	Yes	Not Mentioned	Yes Law Enforcement Agencies Exception	Yes
Delaware	Yes	Yes	Not Mentioned	Yes	Not Mentioned	Yes	Yes	Yes
District of Columbia	Yes	Yes	Not Mentioned	Not Applicable	Not Mentioned	Yes	Not Applicable	Not Applicable
Illinois	Yes	Yes	Yes	Yes	Yes	Not Mentioned	Not Mentioned	Yes
Louisiana	Yes	Yes	Not Mentioned	Yes	No	Yes	Yes	Yes
Maine	Yes	No	Not Mentioned	Yes	Not Mentioned	Not Mentioned	Not Mentioned	Yes
Maryland	Yes	Yes	Yes	Yes	Not Mentioned	Not Mentioned	Yes	Yes
Michigan	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Montana	Yes	Yes	Yes	Yes	Not Mentioned	Not Mentioned	Not Mentioned	Yes
Nebraska	Yes	Yes	Yes	Yes	Yes	Not Mentioned	Yes, Law Enforcement Agencies Exception	Yes
Nevada	Yes	No	Not Mentioned	Yes	Not Mentioned	Not Mentioned	Not Mentioned	Not Mentioned

STATE	Are personal social media accounts covered by the law?	Is personal social media defined?	Is there a private civil right of action?	Are current employees covered by the law?	Are attorneys fees available?	Does the law cover colleges and universities?	Are public employees covered by the law?	Exceptions for investigations of employee misconduct?
New Hampshire	Yes	Yes	Not Mentioned	Yes	Not Mentioned	Not Mentioned	Not Mentioned	Yes
New Jersey	Yes	Yes	Yes	Yes	Yes	Yes	Yes Law Enforcement Agencies Exception	Yes
New Mexico	Yes	No	Not Mentioned	No	Not Mentioned	Yes	Law Enforcement Agencies Are Not, Does Not Mention Other Public Employers	Does Not Apply
Oklahoma	Yes	Yes	Yes	Yes	Not Mentioned	Not Mentioned	Not Mentioned	Yes
Oregon	Yes	Yes	Yes	Yes	Yes	Yes	Not Mentioned	Yes
Rhode Island	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Tennessee	Yes	Yes	Yes	Yes	Yes	Not Mentioned	Yes Law Enforcement Agencies Exception	Yes
Utah	Yes	Yes	Yes	Yes	Not Mentioned	Yes	Yes Law Enforcement Agencies Exception	Yes
Vermont	Yes	Yes	Not Mentioned	Yes	Not Mentioned	Not Mentioned	Yes Law Enforcement Agencies Exception	Yes
Virginia	Yes	Yes	Not Mentioned	Yes	Not Mentioned	Yes	Yes	Yes
Washington	Yes	No	Yes	Yes	Yes	Not Mentioned	Yes	Yes
West Virginia	Yes	Yes	Not Mentioned	Yes	Not Mentioned	Not Mentioned	Not Mentioned	Yes
Wisconsin	Yes	Yes	No	Yes	No	Yes	Yes	Yes

STATE	Is shoulder surfing prohibited?	Must admin. requirements be exhausted before filing suit?	Exceptions for information available on the public domain?	Are employer issued/ business related accounts covered under legislation?	Are employers prohibited from retaliating?	Is there an exception to comply with regulations?	Is there an exception to implement policies on use	Is there an exception to discipline for transfer of confidential info?	Is there an exception to monitor?
Arkansas	Unclear	Not Mentioned	Yes	No	Yes	Yes	Not Mentioned	Not Mentioned	Yes
California	Yes	Not Mentioned	Not Mentioned	No	Yes	Yes	Not Mentioned	Not Mentioned	Not Mentioned
Colorado	Unclear	No	Not Mentioned	No	Yes	Yes	Not Mentioned	Yes	Not Mentioned
Connecticut	Yes	Unclear	Not Mentioned	No	Yes	Yes	Not Mentioned	Yes	Yes
Delaware	Yes	Not Mentioned	Yes	No	Yes	Yes	Not Mentioned	Not Mentioned	Yes
District of Columbia	Yes	Not Mentioned	Yes	Not Applicable	Yes	Not Mentioned	Yes	Not Mentioned	Yes
Illinois	Yes	Not Mentioned	Yes	No	Yes	Yes	Yes	Yes	Yes
Louisiana	Not Mentioned	Not Mentioned	Yes	No	Yes	Yes	Not Mentioned	Yes	Yes
Maine	Yes	Not Mentioned	Yes	No	Yes	Yes	Yes	Not Mentioned	Yes
Maryland	Not Mentioned	Not Mentioned	Not Mentioned	No	Yes	Yes	Not Mentioned	Yes	Not Mentioned
Michigan	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
Montana	Yes	Not Mentioned	Not Mentioned	No	Yes	Yes	Yes	Yes	Not Mentioned
Nebraska	Yes	Not Mentioned	Yes	No	Yes	Yes	Yes	Yes	Yes
Nevada	Not Mentioned		Not Mentioned	No	Yes	Yes	Not Mentioned	Not Mentioned	Not Mentioned

STATE	Is shoulder surfing prohibited?	Must admin. requirements be exhausted before filing suit?	Exceptions for information available on the public domain?	Are employer issued/ business related accounts covered under legislation?	Are employers prohibited from retaliating?	Is there an exception to comply with regulations?	Is there an exception to implement policies on use	Is there an exception to discipline for transfer of confidential info?	Is there an exception to monitor?
New Hampshire	Not Mentioned	Not Mentioned	Yes	No	Yes	Yes	Yes	Yes	Yes
New Jersey	Not Mentioned	Not Mentioned	Yes	No	Yes	Yes	Yes	Yes	Not Mentioned
New Mexico	Not Mentioned	Not Mentioned	Yes	Not Applicable	Not Mentioned	Not Mentioned	Yes	Not Mentioned	Yes
Oklahoma	Yes	Not Mentioned	Yes	No	Yes	Yes	Not Mentioned	Yes	Yes
Oregon	Yes	Not Mentioned	Yes	No	Yes	Yes	Not Mentioned	Not Mentioned	Yes
Rhode Island	Yes	Not Mentioned	Yes	No	Yes	Yes	Not Mentioned	Not Mentioned	Yes
Tennessee	Yes	Not Mentioned	Yes	No	Yes	Yes	Not Mentioned	Yes	Yes
Utah	Not Mentioned	Not Mentioned	Yes	No	Yes	Yes	Yes	Yes	Yes
Vermont	Yes	Not Mentioned	No	No	Yes	Yes	Not Mentioned	Yes	No
Virginia	Not Mentioned	Not Mentioned	Yes	No	Yes	Yes	Yes	Not Mentioned	Yes
Washington	Yes	Not Mentioned	Not Mentioned	No	Yes	Yes	Yes	Yes	Yes
West Virginia	Yes	Not Mentioned	Yes	No	Not Mentioned	Yes	Not Mentioned	Yes	Yes
Wisconsin	Yes	Yes	Yes	No	Yes	Yes	Not Mentioned	Yes	Yes

Notes

Notes

SEYFARTH SHAW

Atlanta
Boston
Chicago
Hong Kong
Houston
London
Los Angeles
Melbourne
New York
Sacramento
San Francisco
Shanghai
Sydney
Washington, D.C.

www.seyfarth.com