AMERICAN BAR ASSOCIATION SECTION OF LABOR AND EMPLOYMENT LAW
EMPLOYMENT RIGHTS AND RESPONSIBILITIES COMMITTEE
Midwinter Meeting
March 19-23, 2013
Miami Beach, Florida

A SURVEY OF STATE LAWS RELATING TO SOCIAL NETWORKING PRIVACY AND OTHER RECENT DEVELOPMENTS IN WORKPLACE PRIVACY LAW

Submitted by:

The State Law Developments Subcommittee

Authors (and states researched by each author):

Wynter Allen (DC, FL, MD, MS, NC, SC, VA, WV)

Tiffanie A. Benfer (AK, CA, ID, MT, NV, NM, OR, UT, WA)

Jeffrey A. Dretler (CT, KY, ME, MA, NH, NY, RI, VT)

Michael D. Homans (AB, AZ, DE, GA, LA, NJ, PA, TX)

Richard A. Hooker and Luis E. Avila (AR, IL, IN, MI, MN, OH, TN, WI)

James Zalewski (CO, IA, KS, MN, MO, NE, ND, OK, SD, WY)

Introduction

Workplace privacy laws, especially those relating to social networking, are among the most active areas of development in state law. This article provides a state-by-state survey of recent legislation enacted to protect employee privacy, as well as a summary of case law developments relating to workplace privacy rights and social networking.

Section I is devoted to developments in state law from approximately 2010 forward, and constitutes the majority of this paper. This survey demonstrates that the current focus is on social media access, password-protected communications, and employer monitoring of employee Internet use. These topics have prompted both state and federal legislatures to place new emphases on employee privacy in the workplace. Courts have weighed in, too, ruling on social

media and electronic communication privacy issues under the common law, where the legislative slate is blank.

Section II consists of a sampling of other state privacy law developments, and is provided simply as a reminder and prompt to practitioners to be aware of, and research as needed, the broad range of state-law protections in the workplace. Readers should understand that Section II is not designed to be comprehensive or consistent from state to state. Rather, it consists of older state law privacy issues that the authors collected as they researched and drafted Section I.

Federal law. Importantly, this paper does not address developments in federal law, statutory or otherwise, relating to employee privacy and social networking. Obviously, substantial federal law and proposed legislation exist on these issues, including without limitation recent National Labor Relations Board rulings and guidance, and various bills pending in Congress, including the proposed Password Protection Act of 2012 and the Social Networking Online Protection Act. The latter died in committee in 2012, but at least one legal eagle has called it the "Frankenstein [that] will come back to life again in the current legislative session." Practitioners are advised to independently assess federal law applications before advising on these issues.

SECTION I

RECENT DEVELOPMENTS IN STATE WORKPLACE PRIVACY LAWS, INCLUDING SOCIAL NETWORKING STATUTES AND BILLS

1. ALABAMA

Alabama has not enacted any new workplace privacy laws, and does not have any laws relating to social media access by an employer. Alabama does not have any pending legislation relating to social media or workplace privacy.

2. ALASKA

Alaska has not enacted any new workplace privacy laws, and does not have any laws relating to social media access by an employer. Currently, Alaska has no pending legislation related to employee privacy and social media.

3. ARIZONA

I. Statutes

Arizona has not enacted any new workplace privacy laws, and does not have any laws relating to social media access by an employer.

II. Pending Legislation

On February 14, 2013, the Senate Public Safety Committee approved S.B. 1411, which prohibits an employer from discharging, disciplining or otherwise penalizing an employee who refuses to provide a social media password. The same protection applies to job applicants.

A bill was introduced in 2012 to prevent "annoying" or "offensive" comments made on Internet sites or sent in text messages. The bill is an amendment to the State's telephone harassment and stalking law, ARS 13-2921.

4. ARKANSAS

I. Statutes

Arkansas has not enacted any new workplace privacy laws, and does not have any laws relating to social media access by an employer. Currently, Arkansas has no reported pending legislation related to employee privacy and social media.

II. Case law developments

A. First Amendment protections relating to social media

Mattingly v. Milligan, 32 IER Cases 1781 (E.D. Ark. 2011) – A former employee of a county clerk's office was found to have a triable free-speech claim under the First Amendment, after she was discharged for posting comments to a social networking web site expressing sympathy for co-workers who were fired when the newly elected clerk took office. Numerous comments responding to the employee on the same website and coverage by news media indicated her speech addressed a matter of public concern, she did not make comments in her capacity as an employee, six telephone calls to clerk's office by constituents who saw the posting did not disrupt the workplace, and the clerk did not have qualified immunity.

5. CALIFORNIA

I. Statutes

A. 2012 law limits employer access to employees' social media accounts

AB 1844

On September 27, 2012, the Governor of California signed into law AB 1844, codified in LAB Div. 2 Part 3 Chapter 2.5 Employer Use of Social Media 980. AB 1844 prohibits private employers from requiring or requesting that an employee or applicant for employment do the following:

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.

The legislature, however, carved out an exception to these requirements. Employers maintain the right and obligation to "request an employee to divulge personal social media reasonably believed to be relevant to an investigation of all allegations of employee misconduct or employee violation of applicable law and

regulations, provided that the social media is used solely for purposes of that investigation or a related proceeding."

The law also specifically states that it does not prohibit an employer from requesting that an employee provide a username, password or other method for the purpose of accessing employer-issued electronic devices.

The law also contains an anti-retaliation provision. It prohibits an 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 by the employer that violates" this new law.

Social Media is defined as an "electronic service or account, or electronic content, including, but not limited to videos, still photographs, blogs, video blogs, podcasts, instant and text messages, email, online services or accounts, or Internet Web site profiles or locations."

The term "personal" appears right before the term "social media" consistently throughout the law, but the legislature failed to define "personal." According to the Merriam-Webster dictionary, the word "personal" means: "of, relating to, or affecting a particular person." Hence, the courts will have to decide whether this new law encompasses email accounts issued by the employer.

II. Pending Legislation

A. Public Employee Privacy

On December 3, 2012, the California Legislature introduced AB 25. The bill extends the same protection provided by AB 1844 to public employees. The bill's provisions apply to public employers generally, including charter cities and counties.

AB 1844 and AB 25 do not place any restrictions on employers viewing social media accounts that are accessible to the public. Therefore, employers may continue to view and use information that is accessible to the public. This would include inappropriate pictures, tweets, and other social media indiscretions.

However, when viewing an employee's or prospective employee's public social media accounts, the employer will most likely be able to obtain personal information relating to race, gender, age, sexual orientation, and disability. Employers should be forewarned that this practice could make them vulnerable to potential liability if it can be established that this information was used to unlawfully discriminate against protected groups.

III. Case law developments

A. Employee Privacy in Regard to Employer Issued Email Accounts (decided prior to AB 1844)-

An employee's right to privacy as it pertains to a company email account was taken under consideration in *Holmes v. Petrovich Dev. Co.,* 191 Cal. App. 4th 1047, 1071, 119 Cal. Rptr. 3d 878, 898 (2011). In *Holmes,* the court held that emails sent by an employee (who sued her boss for sexual harassment, retaliation, and wrongful termination) to her attorney from the company's computer and company email account were not protected by attorney client privilege. The employee argued that the emails were personal; however, the court did not agree and relied heavily upon the company policy in support of its position. The evidence showed that the company explicitly informed employees that they did not have a right to privacy in regard to personal e-mails sent using company computers, and that the company could inspect those e-mails at any time at its own discretion. The court also noted that the company never conveyed a conflicting policy to its employees. The court drew a distinction to the New Jersey Supreme Court's holding in *Stengart v. Loving Care Agency, Inc*., 201 N.J. 300, 990 A.2d 650, 663 (2010), in which the N.J. Supreme Court concluded that an employee had a reasonable expectation of privacy with regard to the personal web-based email sent to her attorney from her employer's computer. This decision provides some insight into the California state court's perspective about email sent from employer's computers and employer-issued email accounts.

B. Employee Privacy as to Personal Email Accounts Accessed on Employer Issued Computer (decided prior to AB 1844)

In *Doe v. City & County of San Francisco*, C10-04700 TEH, 2012 WL 2132398 (N.D. Cal. June 12, 2012), the employer provided a bank of computers for the employees to use on their breaks. Employees could check personal email and use the internet for non-work-related reasons, as long as they did not use the computers for any improper purpose. In October of 2009, the employer printed 28 emails from Jane Doe's personal Yahoo! email account and submitted the emails to the human resources department for review. The employer's actions were allegedly motivated out of concern that the Plaintiff was improperly disclosing confidential personnel information to outside parties. Defendants claimed that the Plaintiff left these emails open in multiple minimized windows on the shared computer. Plaintiff denied that she left the emails open and asserted invasion of privacy. The claim rests on the reasonable expectation of privacy, which "is an objective entitlement founded on broadly based and widely accepted community norms." *Id*. (citing *Sheehan v. San Francisco 49ers, Ltd*., 45 Cal. 4th 992, 1000, 89; Cal. Rptr. 3d 594, 201 P.3d 472 (2009). The court determined "a reasonable jury could conclude that Plaintiff had a legitimate expectation of privacy when she used the terminal to access her personal web-based email."

6. COLORADO

I. Statutes

Colorado has not enacted any new workplace privacy laws, and does not have any laws relating to social media access by an employer.

II. Pending Legislation

Introduced January 9, 2013, HB 13-1046, prohibits an employer from requiring an employee or applicant to disclose a password for a personal account through an electronic communications device. Employers are prohibited from discipline or discharge of an employee who refuses to provide a password.

7. CONNECTICUT

I. Statutes

Connecticut has not enacted any new workplace privacy laws, and does not have any laws relating to social media access by an employer.

II. Case law developments

A. Former employee of University of Connecticut Health Center had no reasonable expectation of privacy in the information stored in her workplace computer which, when retrieved by her employer, ultimately led to her criminal conviction for forgery and larceny. As such, the court denied her habeas corpus petition. *Dickman v. Warden, State Prison*, CV104003480, 2012 WL 527639 (Conn. Super. Ct. Jan. 25, 2012).

B. *Gerardi v. City of Bridgeport*, 294 Conn. 461, 985 A.2d 328 (Conn. 2010) (in what appears to be a case of first impression, holding that the Connecticut electronic monitoring statute creates neither an express nor an implied private right of action that would permit employees to sue their employers for violations of the statute).

8. DELAWARE

I. Statutes

A. Phone, email and Internet monitoring restricted

Del. Code Ann. 19 § 705 provides that a public or private employer may not monitor or otherwise intercept any telephone, email or Internet communication or usage by a Delaware employee unless the employer either: (1) provides an electronic notice of such monitoring or intercepting policies or activities to the employee at least once during each day the employee accesses the employer provided E-mail or Internet access services; or (2) has first given a one-time notice to the employee of such monitoring or intercepting activity or policies. The notice must be in writing, in an electronic record, or in another electronic form and acknowledged by the employee either in writing or electronically. Violators of the law are subject to a civil penalty of $100 for each such violation, in addition to any other remedies available under any other law, or the common law. The law does not apply to processes that are designed to manage the type or volume of incoming or outgoing electronic mail or telephone voice mail or internet usage, that are not targeted to monitor or intercept the electronic mail or telephone voice mail or internet usage of a particular individual, and that are performed solely for the purpose of computer system maintenance and/or protection.

B. Electronic eavesdropping

Del. Code Ann. 19 § 1335 broadly makes it a crime to violate a person's privacy, including multiple specific acts such as "Install[ing] in any private place, without consent of the person or persons entitled to privacy there, any device for observing, photographing, recording, amplifying or broadcasting sounds or events in that place," and "Intercept[ing] without the consent of all parties thereto a message by telephone, telegraph, letter or other means of communicating privately, including private conversation." The law contains numerous exceptions that may apply in workplace settings.

II. Pending Legislation

A. Workplace Privacy Act would protect social media passwords

This bill has been stuck in committee since the summer of 2012, but the Delaware Workplace Privacy Act, House Bill No. 308, has lofty goals, referring to the need to protect the privacy of online social networking, which is "the new digital age 'public square' for important discourse."

The bill would make it unlawful for employers to mandate that an employee or applicant disclose password or account information relating to a social networking profile or account. The bill also would prohibit employers from requesting that employees or applicants log onto their respective social networking accounts to provide the employer with direct access.

The bill includes an exception for employers in the financial services industry conducting internal investigations into employee wrongdoing and compliance. Amendments to the bill also would include exceptions for law enforcement agencies, the Department of Corrections.

A proposed amendment provides that the Act does not limit an employer's ability to bar employees from accessing social networking sites while performing work for the employer, or from accessing electronic communication devices which are the property of the employer. Also, when an employer has credible information indicating imminent workplace violence, the employer would be able to question the subject employee as to alleged social network postings.

9. DISTRICT OF COLUMBIA

The District has not enacted any new workplace privacy laws, and does not have any laws relating to social media access by an employer.

10. FLORIDA

Florida has not enacted any new workplace privacy laws, and does not have any laws relating to social media access by an employer.

11. GEORGIA

I. Statutes

A. Vehicle privacy at work

Ga. § 16-11-135(a) prohibits private and public employers from establishing or enforcing any policy or rule "that has the effect of allowing such employer or its agents to search the locked privately owned vehicles of employees or invited guests on the employer's parking lot."

II. Pending legislation

A. Social media password protection

Georgia House Bill 117 would prohibit employers from requesting or requiring that employees (1) disclose their usernames, passwords or other means of accessing personal accounts on electronic communication devices; (2) access personal social media in the presence of the employer; or (3) divulge any personal social media activity. The bill provides exceptions for situations in which an employer is conducting an investigation of possible misconduct or legal violations and believes that the employee's personal social media activity could be relevant to the investigation (and then can ask the employee to access the social media in the employer's presence, solely for the purposes of the investigation). In addition, the bill would allow employers to access "nonpersonal account" on the employer's own computer or information systems. Violations would be punished with civil fines of up to $400.

House Bill 149 is similar, but would specifically prohibit employers from discharging, disciplining, penalizing, threatening or retaliating against an employee for refusing to comply with the employer's request. If enacted, this bill would allow employees who suffer a violation to recover a civil penalty of $1,000 per violation, plus actual damages and court costs.

III. Case law

A. **Reviewing an employee's private email page not invasion of privacy**

In *Sitton v. Print Direction, Inc.*, 718 S.E.2d 532, 537, 2011 WL 4469712 at *3 (Ga. App. September 28, 2011), the appellate court held that an employee who used a personal laptop at work to conduct business for a competitor did not have an invasion of privacy claim when his employer discovered the open laptop in his office and printed out emails as part of a workplace investigation into suspected wrongful competition by the employee. Reasoned the court:

> Even if Stanton's review of Sitton's e-mails could be seen as "surveillance," it still does not rise to the level of an unreasonable intrusion upon Sitton's seclusion or solitude, because Stanton's activity was "reasonable in light of the situation." Stanton acted in order to obtain evidence in connection with an investigation of improper employee behavior. In the case before us . . . "the company's interests were at stake." Stanton had every reason to suspect that Sitton was conducting a competing business on the side, as in fact he was.

Id. (citations and footnotes omitted).

12. HAWAII

I. Statutes

Hawaii has not enacted any new workplace privacy laws, and does not have any laws relating to social media access by an employer.

II. Pending legislation

A. Social media passwords

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: January 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 intent accounts; provides penalties

S.B. 207: Status: February 12, 2013; In Senate Committee on Technology and the Arts: Voted to pass the amendment. Prohibits employers from requiring employees and applicants for employment from disclosures social media usernames or password.

13. IDAHO

I. Statutes

Idaho has not enacted any new workplace privacy laws, and does not have any laws relating to social media access by an employer.

II. Case Law

A. Employee Privacy and Social Media with Regard to Employer-Issued Email Accounts

In *Cowles Pub. Co. v. Kootenai County Bd. of County Com'rs*, 144 Idaho 259, 265, 159 P.3d 896, 902 (2007), the state's Supreme Court provided limited direction regarding employee privacy and social media. In *Cowles Pub. Co.,* the court considered whether emails sent from an email account provided by the

public employer were private. The court concluded, "under the clear wording of the employer's email policy the Plaintiff had no legitimate expectation of privacy in the emails," because the employer's policy stated, "employees have no right to personal privacy when using the email system(s) provided by the County."

14. ILLINOIS

I. Statutes

A. Surveillance and Eavesdropping

State law generally prohibits the monitoring of telephone conversations, but grants exceptions, with restrictions, to certain businesses for specified activities, such as engaging in marketing, opinion research, telephone solicitation and training, but only so long as the monitoring is used with the consent of at least one person who is an active party to the call. (720 Ill. Comp. Stat. 5/14-3, as amended by 2012 Ill. Laws 97-846, 97-897, both effective Jan. 1, 2013.)

B. Social Media

Effective January 1, 2013, employers are prohibited from demanding access to an applicant's or employee's social media account or profile, or his or her user names or passwords linked to social networking sites. However, an employer is not prohibited from obtaining information that is in the public domain about an applicant or employee. 820 Ill. Comp. Stat. 55/10, as amended by 2012 Ill. Laws 97-875, effective Jan. 1, 2013; and 55/15, as amended by 2009 Ill. Laws 92-623. *But see, Thayer v. Chiczewski*, 2009 WL 2957317 (N.D. Ill., Slip Op. 9-11-2009), in which the federal district court ordered plaintiff to consent to and authorize defendant's access to plaintiff's social media records.

C. Social Security Number and Identity Privacy

The Consumer Fraud and Deceptive Business Practices Act (815 Ill. Comp. Stat. 505/2RR, as amended by 2011 Ill. Laws 97-139, effective Jan. 1, 2012) prohibits employers from, among other things: publicly posting or displaying an employee's Social Security number in any manner; requiring an employee to transmit the Social Security number over the internet unless the number is encrypted and the connection is secure; and encoding or embedding the Social Security number in or on a card or document.

II. Case law

A. Surveillance and eavesdropping

1. *Borchers v. Franciscan Tertiary Province,* 962 N.E.2d 29 (Ill. App. 2012) – An employer who allegedly accessed a former employee's personal e-mail account in order to look for business records violated the Stored Communications Act and intruded upon privacy as a matter of common law by downloading and circulating copies of non-business related personal communications discovered in the search for business records.

2. *Shefts v. Petrakis,* 758 F. Supp.2d 620 (C.D. Ill. 2010) – Where a corporate officer's electronic messages were transmitted via the company's server and the company had openly reserved both the right to access all transmissions in its system and appointed a "security liaison" to monitor the system, the officer was held to have consented to the interception.

3. *Carroll v. Lynch,* 698 F.3d 561 (7th Cir. 2012) – The state's eavesdropping statute's "fear of crime" exemption applied in a situation where the spouse of an employee's co-worker, who recorded the employee's telephone call to the co-worker, had a reasonable suspicion that the employee was committing, was about to commit, or had committed a criminal offense against the co-worker. The worker and the employee's supervisors subsequently used the recording in terminating the employee.

B. Social Media

Maremont v. Susan Friedman Design Group, Ltd., 2011 WL 902444 (N.D. Ill. Mar. 15, 2011) – An employer that allegedly posted to an employee's Facebook and Twitter accounts without her consent may be liable for false association/false endorsement under the Lanham Act, 15 U.S.C. § 1125(a)(1)(A), and the right to publicity under the Illinois Right to Publicity Act.

C. Social Security number and identity privacy

Cooney v. Chicago Pub. Schs., 943 N.E.2d 23 (Ill. App. 2010) – The Chicago School Board accidentally mailed to 1,750 employees the name, address, marital status, and Social Security number of all employees. The city was sued for negligence and violation of a state consumer fraud law regulating the disclosure of Social Security numbers to the "general public." The court found the creation of a duty in regard to such "personal data" to be for the legislature, and the Board of Education was not a "person" within the meaning of the Act. It could not, therefore, be held liable under it. With regard to the invasion of privacy claim, the court chose to apply the Restatement's requirement that the facts disclosed must

be private in the sense of being "embarrassing and highly offensive if disclosed." It concluded that a mere number is incapable of being either.

D. Medical/genetic information

Cooney v. Chicago Pub. Schs., 943 N.E.2d 23 (Ill. App. 2010) – The Chicago School Board accidentally mailed to all 1,750 employees the medical, dental, and health insurance information of all employees. The court dismissed the HIPAA claim finding no duty of non-disclosure on the grounds that HIPAA's protection excludes "employment records held by a covered entity in its role as employer."

15. INDIANA

I. Statutes

A. Surveillance and eavesdropping

In 2010, Indiana stiffened the penalties for violations of the unlawful interception of electronic communications. Under Ind. Code §§ 35-33.5-5-4, employers that illegally intercept electronic communications are guilty of a class C felony punishable by fines of up to $10,000, imprisonment of up to four years, or both. *Also see* Ind. Code §§ 35-50-2-6. Employers also can be sued for damages, court costs, and reasonable attorneys' fees by employees whose privacy rights have been violated in this manner.

II. Case law

A. Surveillance and eavesdropping

Rene v. G.F. Fishers, Inc., 817 F. Supp.2d 1090 (S.D. Ind. 2011) – An employer allowed its employee to access personal e-mail and checking account via its computer. The employer also installed keystroke software that, by recording each keystroke, allowed it to gain access to these accounts. Employee's complaint was held actionable under the Stored Communications Act, regardless of whether the employer actually opened the e-mail. Further, Indiana's electronic interception law merely requires that the interception occur contemporaneously with transmission by a system.

16. IOWA

I. Statutes

Iowa has not enacted any new workplace privacy laws, and does not have any statutes relating to social media access by an employer.

II. Pending Legislation

A Social Media Password Protection bill, HF 127, was introduced on January 29, 2013. In addition to the provisions which prohibit an employer from requiring the disclosure of social media passwords, and non-retaliation, the bill also states an employer may discipline or terminate an employee for transferring computer proprietary information to the employee's personal internet account.

In addition, the bill provides for a monetary penalty of up to $1,000.00 for each violation.

17. KANSAS

I. Statutes

Kansas has not enacted any new workplace privacy laws, and does not have any statutes relating to social media access by an employer.

II. Pending Legislation

House Bill 2092, introduced January, 2013, prohibits employers from requiring applicants or employees to disclose social media passwords. Employers further would be prohibited from discipline or discharge of an employee who refused to do so.

18. KENTUCKY

I. Statutes

Kentucky has not enacted any new workplace privacy laws, and does not have any statutes relating to social media access by an employer.

II. Case law developments

A. Off-duty conduct

The Kentucky Court of Appeals recently decided that an employee's conviction for drug offenses warranted the denial of unemployment benefits, even though his conduct occurred off-duty and away from the employer's premises. Jean v.

Kentucky Unemployment Ins. Comm'n, 2010-CA-001623-MR, 2012 WL 2899599 (Ky. Ct. App. July 13, 2012)

19. LOUISIANA

I. Statutes

La. Code 15:1303 restricts the interception and disclosure of wire, electronic and oral communications. Similarly, La. Code § 14:322 prohibits wire-tapping without consent.

II. Case law developments

Termination of reporter due to social networking response causes public controversy. Although Louisiana does not have a social networking privacy law, a television station there has suffered substantial negative publicity because it terminated a reporter in December of 2012 due to her pointed responses to insulting -- and many believed bigoted and sexist -- viewer comments about her hair and looks on Facebook. A viewer wrote on the Facebook page of local television station KTBS-TV that Lee was a very nice "black lady," but that "she needs to wear a wig or grow some more hair." Lee responded, "I am sorry you don't like my ethnic hair. . . . I am very proud of my African-American ancestry which includes my hair . . . I'm very proud of who I am and the standard of beauty I display. Women come in all shapes, sizes, nationalities, and levels of beauty. Showing little girls that being comfortable in the skin and HAIR God gave me is my contribution to society. Little girls (and boys for that matter) need to see that what you look like isn't a reason to not achieve their goals."

The company did not have a formal policy on responding to social media posts, but had distributed an email memo in August of 2012, advising employees that, "When we see complaints from viewers, it's best not to respond at all." Contrary to this guidance, Lee had more than once responded to viewer comments, and as a result was terminated for "repeatedly violating that procedure," the television station said in published reports.

Supporters of Lee started an on-line petition and had obtained more than 48,000 signatures in support of reinstating Lee as of February of 2013. Although Lee has sued a prior employer in Austin, Texas, for alleged racial treatment, no lawsuit has yet been reported in the Louisiana case.

20. MAINE

I. Statutes

Maine has not enacted any new workplace privacy laws, and does not have any statutes relating to social media access by an employer.

II. Case law developments

Savage v. Maine Pretrial Services, Inc., 58 A.3d 1138 (Maine 2013) (Maine Medical Use of Marijuana Act (MMUMA), which legalized medical marijuana, did not create private right of action for former employee to sue former employer for termination due to legal medical marijuana use).

21. MARYLAND

I. Statutes

A. Social media passwords

In 2012, Maryland became the first state to enact a law prohibiting employers from requiring disclosure of employee user names or passwords to personal social media accounts or services.

Effective: October 1, 2012, the law applies to all private employers in Maryland, as well as the state and local governments, and provides as follows:

(b)(1) Subject to paragraph (2) of this subsection, an employer may not request or require that an employee or applicant disclose any user name, password, or other means for accessing a personal account or service through an electronic communications device.

(2) An employer may require an employee to disclose any user name, password, or other means for accessing nonpersonal accounts or services that provide access to the employer's internal computer or information systems.

(c) An employer may not:

(1) discharge, discipline, or otherwise penalize or threaten to discharge, discipline, or otherwise penalize an employee for an employee's refusal to disclose any information specified in subsection (b)(1) of this section; or

(2) fail or refuse to hire any applicant as a result of the applicant's refusal to disclose any information specified in subsection (b)(1) of this section.

(d) An employee may not download unauthorized employer proprietary information or financial data to an employee's personal Web site, an Internet Web site, a Web-based account, or a similar account.

(e) This section does not prevent an employer:

(1) based on the receipt of information about the use of a personal Web site, Internet Web site, Web-based account, or similar account by an employee for business purposes, from conducting an investigation for the purpose of ensuring compliance with applicable securities or financial law, or regulatory requirements; or

(2) based on the receipt of information about the unauthorized downloading of an employer's proprietary information or financial data to a personal Web site, Internet Web site, Web-based account, or similar account by an employee, from investigating an employee's actions under subsection (d) of this section.

Practice Note: The statute does not contain an enforcement provision, and does not provide for remedies or penalties. An employee who is discharged for failure to disclose a social media password might be able to argue wrongful discharge in violation of public policy. It is unclear whether an employee who is disciplined short of termination would have a claim. Courts have yet to decide if an applicant who is denied employment in violation of the law would be able to assert a claim.

22. MASSACHUSETTS

I. Statutes

A. Criminal Offender Record Information Act

On August 6, 2010, Governor Deval Patrick signed legislation reforming the Criminal Offender Record Information Act ("CORI Act") in Massachusetts, which amended a number of different applicable Massachusetts statutes. The CORI Act provides the mechanism through which employers and other interested parties can access Massachusetts criminal records. The reforms both expand and simplify the ability of employers and others to access information, but also limit the scope of information and impose a number of requirements on employers concerning recordkeeping, obligation to develop and maintain a CORI policy, and more. A few of the more significant changes include the following:

Banning employers from asking, *on an initial written job application*, any information concerning an applicant's criminal history, unless conviction information is required for a particular position under state or federal laws. (Effective November 2010) (emphasis added);

Easing the way in which employers and others can access criminal histories, but limiting the types of information that will be provided (e.g., felony convictions generally only available within the past 10 years and misdemeanor convictions only available within the past 5 years) (Effective May 4, 2012);

Imposes an obligation on employers who make an adverse employment decision based on the criminal history to provide a copy of the record to the applicant or employee (Effective May 4, 2012).

II. Pending legislation

A. Social media password protection

A bill has been proposed in the Massachusetts House of Representatives that would make it unlawful for any employer to ask any employee or prospective employee to provide any password or other related account information in order to gain access to the employee's or prospective employee's account or profile on a social networking website or electronic mail. The bill was filed on March 23, 2012 by Rep. Cheryl A. Coakley-Rivera and is titled *An Act relative to social networking and employment*.

III. Case law developments

A. Tracking employees by GPS

The use of GPS technology to track employees' locations and movements raises significant privacy concerns. Unlike traditional forms of surveillance, GPS can be particularly invasive because of the amount of detail and data that are tracked and the possibility of intruding into an employee's private life. For example, an employer that uses GPS to monitor an employee's use of a company-issued car may track the employee's movements during both personal and business time.

Employers that have attempted to implement GPS monitoring programs often experience significant pushback from employees.

In the case of unionized employers, the use of GPS monitoring may be challenged as an unfair labor practice and an invasion of privacy. *See, e.g.*, *Haggins v. Verizon New England, Inc*., 648 F.3d 50 (1st Cir. 2011) (claims by unionized employees that the requirement that they carry cell phones with GPS devices violated the Massachusetts privacy statute were preempted by collective bargaining agreement; affirming trial court's award of summary judgment for employer due to employees' failure exhaust CBA grievance procedures).

23. MICHIGAN

I. Statutes

A. Social Media

Effective December 28, 2012, employers in Michigan are prohibited from requesting that an employee or applicant grant access to, allow observation of, or disclose information that would allow access to the employee's or applicant's personal internet account. Employers are prohibited from retaliating against employees and applicants for failing to do so. 2012 Mich. Pub. Acts 478 (H.B. 5523). However, employers may request or require employees to disclose access information to, as well as monitor, review, or access electronic data stored in an electronic communications device paid in whole or in part by the employer, or traveling through or stored on an employer's network, in accordance with state and federal laws. *Id.* A violation is a misdemeanor and subjects the employer to a fine. *Id.*

II. Case law

A. Common Law Privacy

Dalley v. Dykema Gossett PLLC, 287 Mich. App. 296, 788 N.W.2d 679 (Mich. App. 2010) – Defendant law firm, acting on a Temporary Restraining Order against Plaintiff's principal for whom Plaintiff acted as an independent contractor from his home, demanded entry to Plaintiff's home and copied 11 hours of electronic data stored on Plaintiff's two computers and hard drives, including all data on a computer Plaintiff identified as containing nothing connected with his work for the principal. Citing *Lewis v. LeGrow*, 258 Mich. App. 175 (2003) and a line of authority establishing Michigan's recognition of the tort of invasion of privacy, the Court of Appeals reversed summary disposition for Defendant and found Plaintiff had stated valid claims for invasion of privacy (intrusion upon seclusion or solitude, or into private affairs) and trespass.

B. Surveillance and eavesdropping

1. *Howell Educ. Ass'n v. Howell Bd. Of Educ.,* 30 IER Cases 594 (Mich. App. 2010) – Employees' consent to school district policy, which notified users of its computer system that school officials may view their e-mail and that documents may be released pursuant to subpoena, did not render their personal union-related e-mails subject to a Michigan FOIA request. The policy did not indicate that users' e-mails could be viewed by any member of public, and the employees' violation of district policy by sending personal communications that were not in furtherance of official district functions supports the conclusion the communications were not a public record.

2. *Kiessel et. al. v. Leelanau County Sheriff et. al.*, No. 1:09-cv-00179-JTN (W.D. Mich., Slip Op. 11/23/10) – Defendants had installed a telephone recording system in the Sheriff's Department Offices and proceeded to monitor and record Plaintiff's conversations without distinction based on the nature of the calls. Plaintiffs brought a multi-count suit alleging violation of the federal Wire and Electronic Communications Interception Act, the 1st, 4th and 14th Amendments of the U.S. Constitution, Michigan's Wire Tapping Statute, Michigan's Whistleblowers' Protection Act and Michigan's Employee Right to Know Act, as well as a common law invasion of privacy claim. Defendants' motion for summary disposition four of the claims were denied and the case was ordered to trial.

C. Social Media

Flagg v. City of Detroit, 252 F.R.D. 346 (E.D. Mich. 2008) – Because the Stored Communications Act prohibits a service provider (here, Facebook) from disclosing Plaintiff's information without her consent, the District Court ordered Plaintiff to provide Defendant with a consent and authorization form directing provider to permit Defendant access to her records, including deleted records.

24. MINNESOTA

I. Statutes

Minnesota has not enacted any new workplace privacy laws, and does not have any statutes relating to social media access by an employer.

II. Pending legislation

A. Social network passwords

H.F. 2963 - Status: March 26, 2012. To House Committee on Commerce and Regulatory Reform. Regular session adjourned. Prohibiting employers from requiring social network passwords as a condition of employment.

H.F. 2982 - Status: March 29, 2012. To House committee on Commerce and Regulatory Reform. Regular session adjourned. Prohibits employers from requesting or requiring social network user names, passwords, or related information.

H.F. 2565 - Status: March 27, 2012. To Senate Committee on jobs and Economic Growth. Regular session adjourned. Prohibits employers from requiring social network passwords as a condition of employment.

25. MISSISSIPPI

Mississippi has not enacted any new workplace privacy laws, and does not have any statutes relating to social media access by an employer.

26. MISSOURI

I. Statutes

Missouri has not enacted any new workplace privacy laws, and does not have any statutes relating to social media access by an employer.

II. Pending legislation

A. Social network passwords

H.B. 2060 - Status: April 30, 2012. To House Committee on Rules. Regular session adjourned. Prohibits an employer from requesting or requiring an employee or applicant to disclose any user name, password, or other means for accessing a personal account or service through electronic means.

Amended version introduced this year as S.R. 164. In addition, employers can require employees to disclose passwords used on social media sites from electronic devices supplied by the employer. The bill was passed on to the General Laws Committee on February 26, 2013.

27. MONTANA

Montana has not enacted any new workplace privacy laws, and does not have any statutes relating to social media access by an employer.

28. NEBRASKA

I. Statutes

A. Social Security number

An employer cannot require an employee to transmit more than the last 4 digits of his or her Social Security Number over the Internet unless the connection is secure, or the information is encrypted. Neb. Rev. Stat. §48-237(2)(b).

II. Pending legislation

A. Social network passwords

Status: Bill introduced on January 10, 2013, to prohibit an employer from requiring an employee to disclose social network passwords. LB 58.

29. NEVADA

I. Statutes

Nevada has not enacted any new workplace privacy laws, and does not have any statutes relating to social media access by an employer.

Effective October 1, 2011, A.B. 211 added Gender Identity/Expression to the employment discrimination statute . Employers may not discriminate against a prospective or current employee based on gender identity/expression. Note: state law already prohibits discrimination based on sexual orientation.

30. NEW HAMPSHIRE

I. Statutes

New Hampshire has not enacted any new workplace privacy laws, and does not have any statutes relating to social media access by an employer.

II. Proposed legislation

A. Social media passwords

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.

III. Case law developments

Employee of medical center who was also a patient of the medical center could sustain cause of action for invasion of privacy against her physician and the

employer for failing to maintain the confidentiality of her medical records which resulted in other employees learning that she tested positive for herpes. Hudson v. Dr. Michael J. O'Connell's Pain Care Ctr., Inc., 822 F. Supp. 2d 84, 97 (D.N.H. 2011)

31. NEW JERSEY

I. Statutes

New Jersey has not enacted any new workplace privacy laws, and does not have any statutes relating to social media access by an employer.

II. Pending legislation

A. Bill Prohibiting Employer Mandate on Social Media Access Awaits Governor's Signature

On October 25, 2012, a unanimous New Jersey Senate approved Act 2878, which would prohibit all New Jersey employers from requiring a current or prospective employee to "provide or disclose any user name or password, or in any way provide the employer access to, a personal account or service through an electronic communication device." The bill also prohibits employers from inquiring as to whether a current or prospective employee has a social networking account or profile.

The bill also prohibits retaliation. An aggrieved individual could file suit and obtain injunctive relief, compensatory and consequential damages, and attorneys' fees and costs. The bill also provides for a civil penalty of up to $1,000 for the first violation and $2,500 for each subsequent violation, collectible by the New Jersey Commissioner of Labor and Workforce Development.

The New Jersey General Assembly previously approved the bill by a 76-1 margin, and it now awaits the signature of Gov. Chris Christie.

III. Case law developments

A. 'High threshold' to establish invasion of privacy claim

In New Jersey, "[t]he right of privacy has been defined as 'the right of an individual to be ... protected from any wrongful intrusion into his or her private life which would outrage or cause mental suffering, shame or humiliation to a person of ordinary sensibilities." *Villanova v. Innovative Investigations, Inc*., 420 N.J. Super. 353, 360 (quoting *Burnett v. Cnty. of Bergen*, 402 N.J. Super. 319, 332, 954 A.2d 483 (App.Div.2008). However, "[a] high threshold must be cleared

to assert a cause of action based on the [common law tort of intrusion on seclusion]. A plaintiff must establish that the intrusion 'would be highly offensive to the ordinary reasonable man, as the result of conduct to which the reasonable man would strongly object.'" *Stengart v. Loving Care Agency, Inc*., 201 N.J. 300, 316, 990 A.2d 650 (2010).

B. Coercing co-worker to show Facebook postings could invade privacy

In two separate decisions, New Jersey courts have recognized that an employee states a case for invasion of privacy if he or she alleges the employer accessed the employee's non-public social media postings without consent.

In *Ehling v. Monmouth-Ocean Hospital Service Corp.*, 872 F. Supp. 2d 369 (D.N.J. May 30, 2012), Judge Martini refused to dismiss a common law invasion of privacy claim against a hospital where the plaintiff alleged that the employer's manager gained the access by "coerc[ing], strongarm[ing], and/or threaten[ing]" a co-worker friend of the plaintiff "into accessing his Facebook account on the work computer in the supervisor's presence." Despite the fact that the plaintiff had knowingly disclosed her Facebook postings to an undetermined number of Facebook "friends," the court found that she had stated a plausible claim for invasion of privacy, "especially given the open-ended nature of the case law" on the point. The court did dismiss a count under the New Jersey Wiretapping and Electronic Surveillance Control Act, N.J.S.A. 21A156A-27, as the Facebook postings were not intercepted in the "course of transmission."

Similarly, in *Pietrylo v. Hillstone Rest. Group*, 2008 U.S. Dist. LEXIS 108834, at *20 (D.N.J. July 24, 2008), the employees prevailed against the employer's efforts to dismiss their invasion of privacy claim based on management's alleged coercion of a co-employee to gain access to a private social media chat room in which the plaintiffs made derogatory statements about their employer and management. The plaintiffs in that case ultimately prevailed in a jury trial.

C. Employee has privacy claim based on employer accessing private emails to lawyer

In *Stengart v. Loving Care Agency, Inc.*, 201 N.J. 300 (2010), the court ruled in favor of an employee's claim that her private emails with her lawyer, which had been captured on workplace computers, were protected by state privacy law.

The court held that the plaintiff, Marina Stengart, had a reasonable expectation of privacy in emails she exchanged with her attorney through her web-based personal email account, even though Stengart had used her employer-issued computer to send the emails. Images of the emails had been saved by the employer's monitoring system. When Stengart sued Loving Care Agency, after leaving employment there, the company recovered the emails from the laptop and

sought to use them in the litigation. The court agreed with Stengart that the email exchanges with her attorney were private.

The Court found that the boilerplate notices in the company's email policy regarding employer access to such communications were insufficient to terminate the employee's privacy rights because the policy did not specifically inform employees that the company stored and could retrieve copies of employees' private web-based emails.

Potential sanctions to employer's attorney: Moreover, the court held that the employer's counsel violated Rule 4.4(b) of the New Jersey Rules of Professional Conduct regarding documents inadvertently sent to a lawyer, by failing to stop reading the private attorney-client e-mail messages and returning them to the employee, once it became apparent to the employer's counsel that these were privileged communications not intended to be disclosed.

32. NEW MEXICO

New Mexico has not enacted any new workplace privacy laws, and does not have any statutes relating to social media access by an employer. New Mexico has no pending legislation related to employee privacy and social media.

33. NEW YORK

I. Statutes

New York has not enacted any new workplace privacy laws, and does not have any statutes relating to social media access by an employer.

II. Proposed legislation

S.B. 6831 **Status**: March 27, 2012. Introduced. 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.

S.B. 6938 **Status**: April 13, 2012. To Senate Committee on Labor. Protects the privacy of employees' and prospective employees' social media accounts.

S.B. 7077 **Status**: May 31, 2012. Amended in Senate Committee on Labor. Protects the privacy of employees' and prospective employees' social media accounts.

A.B. 10396 **Status**: May 31, 2012. Enacting clause stricken. Protects the privacy of employees' and prospective employees' social media accounts.

A.B. 9654 **Status**: June 18, 2012. To Senate Committee on Rules. Same text as S.B. 6831.

III. Case law developments

1. Department of Education's (DOE) decision not to withhold unredacted Teacher Data Reports (TDRs) from public disclosure under Freedom of Information Law (FOIL) exception for inter-agency or intra-agency materials that were not statistical or factual tabulations was not arbitrary or capricious; DOE could have rationally determined that, although the unredacted TDRs were intra-agency records, they were statistical tabulations of data which had to be released under the FOIL. *Mulgrew v. Bd. of Educ. of City Sch. Dist. of City of New York*, 31 Misc. 3d 296, 919 N.Y.S.2d 786 (Sup. Ct. 2011) *aff'd*, 87 A.D.3d 506, 928 N.Y.S.2d 701 (2011) *leave to appeal denied*, 18 N.Y.3d 806, 963 N.E.2d 792 (2012).

2. *United States v. Meregildo*, 883 F. Supp. 2d 523 (S.D.N.Y. 2012) (government did not violate Fourth Amendment when it accessed defendant's profile on social networking website through cooperating witness).

3. *Cunningham v. New York State Dept. of Labor*, 89 A.D.3d 1347, 1350, 933 N.Y.S.2d 432, 436 (2011) (installation of GPS on a state employee's car upheld as reasonable where Inspector General was investigating a pattern of abuse of work time through use of the employee's personal vehicle during work hours).

4. Company stated causes of action under Electronic Communications **Privacy** Act (ECPA), Stored Wire and Electronic Communications Act (SECA), and invasion of privacy, among others, against two former employees who allegedly accessed former employer's emails without authorization. *MidAmerica Productions, Inc. v. Derke*, 33 Misc. 3d 1209(A), 939 N.Y.S.2d 741 (Sup. Ct. 2010).

5. *People v. Klapper*, 28 Misc. 3d 225, 233, 902 N.Y.S.2d 305, 312 (Crim. Ct. 2010) (court dismissed criminal charges against employer/defendant for unauthorized use of computer, even though evidence suggested that employer installed key stroke tracking software on the computer and then was later seen accessing the computer, where the charging instrument did not contain sufficient facts to demonstrate that the employer, who owned the computer, accessed the employee's email without authorization and there was no evidence as to which email account he accessed (work or personal). The court made the following strong observation about an employee's diminished expectation of privacy in emails at work:

> Whereas, some may view emails as tantamount to a postal letter which is afforded some level of privacy, this court finds, in general, emails are more akin to a postcard, as they are less secure and can easily be viewed by a passerby. Moreover, emails are easily intercepted, since the technology of receiving an email message from the sender, requires travel through a network, firewall, and service provider before reaching its final destination, which may have its own network, service provider and firewall. An employee who sends an email, be it personal or work related, from a work computer sends an email that will travel through an employer's central computer, which is commonly stored on the employer's server even after it is received and read. Once stored on the server, an employer can easily scan or read all stored emails or data. The same holds true once the email reaches its destination, as it travels through the internet via an internet service provider. Accordingly, this process diminishes an individual's expectation of privacy in email communications

Id. at 231, 902 N.Y.S.2d at 310-11.

34. NORTH CAROLINA

North Carolina has not enacted any new workplace privacy laws, and does not have any laws relating to social media access by an employer. Currently, North Carolina has no pending legislation related to employee privacy or social media.

35. NORTH DAKOTA

North Dakota has not enacted any new workplace privacy laws, and does not have any laws relating to social media access by an employer. Currently, North Dakota has no pending legislation related to employee privacy or social media.

36. OHIO

I. Statutes

Ohio has not enacted any new workplace privacy laws, and does not have any laws relating to social media access by an employer.

II. Pending Legislation

S.B. 45 was introduced on February 19, 2013, as an amendment to Ohio's Civil Rights Law. It prohibits employers from penalizing employees or applicants for refusing to supply a social media or private electronic password. Such action would be deemed an unlawful discriminatory practice, subject to monetary penalties of $1,000.00 for the first violation, and $2,000.00 for each subsequent violation.

III. Case law developments

A. Social Media

Howell v. Buckeye Ranch, Inc., 34 IER Cases 717 (S.D. Ohio 2012) – The court denied the employer's motion to compel an employee pursuing sexual harassment claim to give user names and passwords for each of her social media sites. The employer claimed these were relevant to whether sexual harassment had occurred, as well as the employee's emotional state. The court found requests for access to all information in private sections of her social media accounts were overbroad.

B. Drug Testing

Palmer v Cacioppo, 429 Fed. Appx. 491, 113 F.E.P. Cases 36 (6th Cir. 2011) – Mandatory drug testing, including random testing, does not violate a Plaintiff's 4th Amendment rights when implemented pursuant to an individual last chance agreement following Plaintiff's misdemeanor conviction for possession of an illegal substance.

37. OKLAHOMA

Oklahoma has not enacted any new workplace privacy laws, and does not have any statutes relating to social media access by an employer.

38. OREGON

I. Statutes

Oregon has not enacted any new workplace privacy laws, and does not have any laws relating to social media access by an employer.

II. Pending Legislation

S.B. 499, introduced in January, 2013, would prohibit an employer from requiring an employee or applicant to produce and disclose any social media password.

The employer is prevented from any form of discipline or retaliation for the employee's refusal to do so.

39. PENNSYLVANIA

I. Statutes

Pennsylvania has not enacted any new workplace privacy laws, and does not have any laws relating to social media access by an employer.

II. Pending legislation

A. Bill Would Ban Employer Requests for Social Media Access

In 2012, legislators have proposed the Social Media Privacy Protection Act, which would prohibit all employers in the Commonwealth from requesting or requiring "that an employee or prospective employee disclose any user name, password or other means for accessing a private or personal social media account, service or Internet website." An employee could not be discharged, disciplined or otherwise penalized for refusing to disclose information protected under the Act. Likewise, an employer could not fail or refuse to hire a prospective employee for refusing to provide such information.

The Pennsylvania bill provides that it does not restrict an employer's right to promulgate and enforce workplace policies governing the use of the employer's electronic communication devices, or the employer's right to monitor the usage of the employer's electronic communication devices, so long as the employer does not request or require employees to provide social media access information. The bill also expressly provides that nothing in the law would limit an employer's right to obtain or view information that exists within the public domain.

An employer that violates the law would be subject to a civil penalty of up to $5,000, in addition to reimbursement of reasonable attorneys' fees.

III. Case law developments

A. Employee's right to LinkedIn page may be protected by privacy, other laws

In *Eagle v. Morgan*, 2012 WL 4738986 (Slip Copy) (E.D. Pa. Oct. 4, 2012), plaintiff Linda Eagle established that she used her LinkedIn account to promote her employer, Edcomm, to foster her own reputation as a businesswoman, and to reconnect with family, friends and colleagues. Edcomm generally recommended that all employees establish LinkedIn accounts listing Edcomm as their employer,

and followed a policy that when an employee left the company, the company would effectively "own" the LinkedIn account and begin mining it for information. After Edcomm terminated Eagle, it used her password to access her account, changed the password so that she could no longer access it, and changed her account, to display the new interim CEO's name and photograph. As a result, Eagle alleged she lost business contacts and potential customers. Among the 11 counts in her federal complaint were invasion of privacy by misappropriation of identity and misappropriation of publicity. The court dismissed Eagle's federal claims under the Computer Fraud and Abuse Act and the Lanham Act, but allowed the state law claims to continue in federal court (the employer had not moved to dismiss those state claims).

40. RHODE ISLAND

I. Statutes

Rhode Island has not enacted any new workplace privacy laws, and does not have any laws relating to social media access by an employer.

II. Pending legislation

A. Social media passwords

House Bill 2013-H5255 was introduced Feb. 5, 2013. It would prohibit employers from requiring an employee or applicant to disclose personal social media information students. It also would protect students.

Under the bill, employers could not require or request that an employee or applicant disclose personal social media information, such as a user name, password or any other means for accessing a personal social media account. An employer also would not be able to compel an employee or applicant to access a personal social media account in the presence of the employer or to add anyone, including the employer or an agent, to the employee's or applicant's list of contacts associated with the social media account, or to change the privacy settings for the account.

Employers could require an employee to divulge personal social media information when it is reasonably believed to be relevant to an investigation of allegations of employee misconduct or an employee violation of law.

The bill also prohibits retaliation against employees or applicants for refusing to divulge social media information protected by the law.

Aggrieved individuals could file a civil action, and obtain injunctive relief, in addition to punitive and actual damages.

III. Case law developments

1. *DaPonte v. Ocean State Job Lot, Inc.*, 21 A.3d 248, 252-53 (R.I. 2011) (former employee could not sustain invasion of privacy action against former employer based on president's removing a misplaced price sticker from a rug and forcefully attaching it to **employee's** shoulder while walking the store with **employee; employee** failed to establish that she threw about her person a seclusion that would merit an expectation of **privacy protected by Rhode Island's privacy statute,** R.I. Gen. Laws § 9-1-28.1.)

2. Current and former **employees** of city police and fire departments brought action against city, director of city's department of communications, and chief of operations in the department of communications, alleging that defendants were responsible for putting a system in place that recorded all telephone calls into and out of the complex (emergency and all other calls) which housed the police and fire departments and that the recordings violated the Fourth Amendment, Rhode Island's equivalent constitutional provision, the federal wiretap statute, Rhode Island's wiretap laws, and the state's privacy act. The First Circuit reversed the trial court's findings of liability against the defendants as to the 4th Amendment claim based on qualified immunity, reversed the trial court's finding of liability against the city under the wiretap laws as the city was not a "person" who could be sued under the wiretap laws and remanded for new trial the judgments against the individuals for violation of the state wiretap and privacy act claims due to error in the verdict form. *See Walden v. City of Providence, R.I.*, 596 F.3d 38, 63 (1st Cir. 2010) (current and former employees may pursue wiretap and invasion of privacy claims against individuals who authorized recording of all calls in the workplace).

41. SOUTH CAROLINA

I. Statutes

South Carolina has not enacted any new workplace privacy laws, and does not have any laws relating to social media access by an employer.

II. Pending legislation

A. Social media passwords

2012 House Bill-H.B. 5105 (Status: March 29, 2012. To House Committee on Judiciary). Provides that an employer may not ask an employee or prospective

employee to provide a password or other related account information in order to gain access to the employee's or prospective employee's profile or account on a social networking website. The refusal of an employee or prospective employee to provide a password, account information, or access to his account or profile on a social networking website to an employer must not be the basis of personnel action including, but not limited to, employment, termination, demotion, or promotions of the employee.

42. SOUTH DAKOTA

South Dakota has not enacted any new workplace privacy laws, and does not have any laws relating to social media access by an employer.

43. TENNESSEE

I. Statutes

Tennessee has not enacted any new workplace privacy laws, and does not have any laws relating to social media access by an employer.

II. Case law developments

A. Surveillance and Eavesdropping

Expert Janitorial LLC v. Williams, 30 IER Cases 1003 (E.D. Tenn. 2010) – Employer stated a claim against former employees under Stored Communications Act where employees allegedly obtained and retained e-mail user names and passwords of the employer's senior employees stored on its computers, and, without authorization, used this information to access the senior employees' e-mail accounts. The Act only requires that the employer be "a facility through which an electronic communication service is provided" and the employer's computers on which data was stored may constitute a "facility" under the Act. Further, under both the Tennessee Wiretapping Act and the Federal Wiretapping Act, anyone who without authorization intercepts an e-mail, or any other wire, oral or electronic communication, violates the wiretap acts only if the e-mail communication is "acquired during the flight of the communication" or "in its split second of transmission over a computer network."

B. Drug Testing

Smith County Ed. Ass'n. v. Smith County Bd. of Ed., 781 F. Supp.2d 604 (M.D. Tenn. 2011) – Plaintiff teachers and their authorized representative filed a Fourth Amendment challenge to Defendant's drug testing policy, which involved

urinalysis. While finding that such policies were often justified and not unconstitutional *per se*, even if they included a random testing element, the District Court struck down Defendant's policy because: i) Defendant had not given adequate notice of either the random testing aspect or the specific drugs covered by the testing; ii) Defendant's policy made it a violation to report for work "while possessing in his/her body, blood, or urine, illegal drugs *in any detectable amount*," and gave Plaintiffs no clear notice of standards or cut-offs; and iii) the manner of testing, i.e., requiring Plaintiffs to line up outside the test facility and splitting samples given in the presence of others to be tested, was unusually invasive and therefore, an invasion of Plaintiffs' privacy interests.

44. TEXAS

I. Statutes

Texas has not enacted any new workplace privacy laws, and does not have any laws relating to social media access by an employer.

II. Pending legislation

Texas House Bill 318 and an identical Senate Bill 118 would "prohibit employers from requiring or requesting access to personal accounts of employees or job applicants through electronic communication devices." The proposal would cover personal cell phones, computers and social media accounts, such as Facebook or Twitter. Other bills introduced in Texas with similar provisions include House Bill 451 and Senate Bill 416. An employer is not prohibited from maintaining lawful workplace policies regarding employee use of employer-provided electronic communication devices, monitoring employee use of employer-provided electronic devices or employer-provided email accounts, or obtaining information that is in the public domain or otherwise lawfully obtained.

III. Case law developments

A. Termination due to Facebook posts regarding work not actionable intrusion on privacy.

In *Roberts v. CareFlite*, Texas Court of Appeal 2d District, No. 02-12-00105-cv (Oct. 4, 2012), paramedic Janis Roberts posted comments to her "friends" on Facebook about her job, including that "she wanted to slap the patient" on a recent helicopter transport. A co-worker saw the posts and reported them to a compliance officer at CareFlite, who warned Roberts that "the public sees your posts. . . . I'm trying to help you realize that people out there are losing their jobs and livelihood because of such posts and I don't want to see that happen to you." Roberts responded, *inter alia*, "Yeah, whatever. YOU weren't there." Roberts

was subsequently fired for her posts about wanting to slap a patient and her "unprofessional and insubordinate" response to the compliance officer.

She sued for invasion of privacy under Texas tort law. The Texas appellate court held that she could not show an intentional intrusion on her privacy that was "highly offensive to a reasonable person." Roberts argued that "[t]he rights of CareFlite employees to discuss in private the issues of patient restraints which affected their safety" somehow supported her invasion of privacy claim and outweighed the employer's concerns as to the public's confidence in the ambulance company. She also argued that the NLRB's recent rulings to protect concerted workplace-related discussions on Facebook somehow supported her invasion of privacy claim. The appellate court found, as the lower court had, that Roberts failed to produce evidence to meet her burden to show "(1) an intentional intrusion, physically or otherwise, upon another's solitude, seclusion, or private affairs or concerns, which (2) would be highly offensive to a reasonable person."

45. UTAH

Utah has not enacted any new workplace privacy laws, and does not have any laws relating to social media access by an employer.

46. VERMONT

I. Statutes

Vermont has not enacted any new workplace privacy laws, and does not have any laws relating to social media access by an employer.

II. Case law developments

1. Employment Security Board (ESB) reasonably determined that claimant's off-duty, off-premises criminal conduct in groping a young woman's breasts and vaginal area over her clothing was not "gross misconduct" connected with claimant's work cleaning certain work areas in hospital, and thus did not completely disqualify him from unemployment compensation benefits when he was discharged for that criminal conduct. *Mohamed v. Fletcher Allen Health Care*, 2012 VT 64, 58 A.3d 222 (Vt. 2012)

2. *Wyatt v. City of Barre/Barre City Fire, Dept.*, 2:11-CV-00297, 2012 WL 1435708 (D. Vt. Apr. 25, 2012) (female firefighter whose employment was terminated for lying after she denied having left an anonymous voice-mail with the State's Emergency Medical Services questioning the fitness for duty of a colleague who had sexually harassed her could not maintain cause of action for

invasion of privacy action against firefighters who listened to the voice-mail and identified her voice as she had waived any right to privacy by leaving the voice-mail in the first instance).

47. VIRGINIA

I. Statutes

Virginia has not enacted any new workplace privacy laws, and does not have any laws relating to social media access by an employer.

II. Case law developments

A. No privacy in stored emails, relying heavily on employer policy

In *U.S. v. Hamilton*, 778 F. Supp. 2d 651 (E.D. Va. 2011), the court held that a public school employee lacked an objectively reasonable expectation of privacy in stored emails following the school's publication of a policy that employee's computers were subject to inspection, although the emails in question were sent prior to the school's implementation of its policy limiting workplace computer privacy.

48. WASHINGTON

I. Statutes

Washington has not enacted any new workplace privacy laws, and does not have any laws relating to social media access by an employer.

II. Pending legislation

A. Social media passwords

S.B. 6637 Status: April 11, 2012, by resolution, reintroduced and retained in present status.

The proposed legislation states the following:

> Any person, firm, corporation, or the state of Washington, its political subdivisions, or municipal corporations to require, directly or indirectly, as a condition of employment or continued employment, that any employee or prospective employee submit any password or other related

account information in order to gain access to the employee's or prospective employee's account or profile on a social networking web site or to demand access in any manner to an employee's or prospective employee's account or profile on a social networking web site.

This proposed legislation is more narrowly constructed than California AB 1844 because it only limits an employer's access to an employee's "social networking web site" rather than "social media." The term "social media" encompasses a broad range of social networking avenues including not only websites but also email, text messages, etc. The phrase "social network web site" only pertains to web sites such as Facebook, LinkedIn and Twitter.

49. WEST VIRGINIA

I. Statutes

West Virginia has not enacted any new workplace privacy laws, and does not have any laws relating to social media access by an employer.

II. Case law developments

A. Public employer's random drug test of employee violated Fourth Amendment

American Federation of Teachers v. Kanawha County Board of Education, 592 F. Supp. 2d 883 (S.D. W.Va. 2009). The questions before the court were whether the random drug testing policy enacted by the board as a state actor violated the Fourth Amendment, W. Va. Const. art. III, § 6, and the right to privacy. The evidence did not demonstrate either that the employees had a reduced expectation of privacy by virtue of their employment in a public school or that there was a special governmental need to guard against a concrete risk of great harm. Therefore, the safety justification offered by the board did not outweigh the privacy interests of the school employees and the board could not abandon the Fourth Amendment's protection against suspicionless searches.

50. WISCONSIN

I. Statutes

A. Medical / Genetic Information

1. The Wisconsin Fair Employment Act, which applies to employers, employment agencies, labor unions, and licensing agencies, prohibits job discrimination against employees on the basis of, among other things, genetic testing. Per the Act, genetic testing may not be used by employers unless an employee requests in writing that such a test be administered to investigate a worker's compensation claim or determine the worker's susceptibility or level of exposure to potentially toxic substances in the workplace. Wis. Stat., Ch. 111, Sec. 111.31, as amended by Act 219, L. 2011, effective April 20, 2012.

2. The Wisconsin law on AIDS testing prohibits employers from requiring that employees or prospective employees undergo testing for the human immunodeficiency virus (HIV), which causes acquired immunodeficiency syndrome (AIDS). The law also forbids employer-employee agreements in which the employer offers extra pay or benefits to induce the employee to take an AIDS test. Wis. Stat. Ann., Ch. 103, Sec. 103.15, as amended by Act 209, L. 2010.

B. Social media passwords

Wisconsin has not enacted any new workplace privacy laws, and does not have any laws relating to social media access by an employer.

II. Case law developments

A. Surveillance and Eavesdropping

1. *Schill v. Wisconsin Rapids Sch. Dist.*, 30 IER Cases 1829 (Wis. 2010) – Teachers' personal e-mail messages sent or received on their work computers and stored on school district's computer network are not public records under Wis. Stat. §19.32(2), where (1) legislature's statement of intent indicates that document must be related to government function in order to be "record"; (2) closely related statutes, executive branch interpretations, and legislative history support the conclusion that e-mails containing solely personal content are not "records"; 3) no other state discloses government employees' personal e-mails under its open-records act; and (4) to exclude personal e-mails does not impose unreasonable burden upon custodian of records.

2. *Hutchins v. Clarke*, 661 F.3d 947 (7th Cir. 2011) – Deputy Sheriff Hutchins, called into an on-air popular radio show and discussed Sheriff Clarke's avoidance of certain African-American groups. Clarke responded by stating, on air, that Hutchins held a grudge due to a disciplinary action for sexual harassment taken by him a few years earlier. The court found Wisconsin's Open Records Law does not apply to the sheriff's oral reference to the deputy's disciplinary record during a phone call to a radio show. The law only provides that with regard to a record containing information about an employee's disciplinary history, if the authority decides to permit access to the requested record, the authority shall serve written notice on the employee. Wis. Stat. § 19.356(2)(a). Similarly, the court found the sheriff did not violate Wisconsin's Right of Privacy statute after applying a balancing test to Hutchins' disciplinary file and finding that there is no genuine public interest in keeping the record closed to the public.

B. Social Security Number and Identity Privacy

State v. Baron, 2009 WI 58, 769 N.W.2d 34 (Wis. 2009) – Defendant used his supervisor's computer password to access the supervisor's files, found e-mails evidencing an extramarital affair, and published them to members of the general public. The following day, the supervisor committed suicide, and Defendant was charged with violating Wis. Stat. 943.201(2)(c), which prohibits identity theft. The trial judge ruled the statute an unconstitutional impingement on Defendant's right of free speech, but both the Court of Appeals and the Supreme Court ruled to the contrary, finding the statute's prohibition on unauthorized access to use of personal identifying information "to harm the reputation" of the other person was narrowly tailored and passed constitutional muster.

51. WYOMING

Wyoming has not enacted any new workplace privacy laws, and does not have any laws relating to social media access by an employer.

SECTION II

A SAMPLING OF OTHER STATE LAWS ON WORKPLACE PRIVACY

This section provides examples of state law privacy issues other than (1) social networking, (2) recently enacted state laws, and (3) recent case law developments in privacy issues. **This section is not intended to be a comprehensive survey of all privacy-related laws,** but rather simply highlights some examples of other privacy-related state laws not included in Section I.

ALABAMA

Eavesdropping

Alab. § 13A-11-31 provides that a "person commits the crime of criminal eavesdropping if he intentionally uses any device to eavesdrop, whether or not he is present at the time."

ALASKA

Drug and Alcohol Test Results

AS § 23.10.660. Confidentiality of results; access to records. A communication received by an employer relevant to drug test or alcohol impairment test results and received through the employer's testing program is a confidential and privileged communication and may not be disclosed except: (1) to the tested employee or prospective employee or another person designated in writing by the employee or prospective employee;

(2) to individuals designated by an employer to receive and evaluate test results or hear the explanation of the employee or prospective employee; or (3) as ordered by a court or governmental agency.

ARKANSAS

Medical / Genetic Information

Arkansas has a Genetic Information in the Workplace Act enacted in 2001. Title 11, Ch. 5, Sec. 11-5-401, Act. 1407, L. 2001.

ARIZONA

Wiretapping, eavesdropping.

Ariz. § 13-3005 makes it a crime to intentionally intercept a conversation or wire or electronic communication to which the interceptor is not a party, except as otherwise provided in the statute.

CALIFORNIA

Statutes – Employee Privacy

Cal. Labor Code § 96. In addition to AB 1844, Cal. Labor Code § 96 (k) prohibits employers from disciplining employees for activity on social networking sites that occurs while the employee is off-duty, unless the employer can demonstrate that the activity can damage the company in some way.

Recent Application of California State Provisions that Grant an Employee Right to Privacy. In California, employees have brought claims against their employers for invasion of privacy under the California Constitution, Cal. Const. art. 1, §1. Under such claims, a plaintiff must show: 1) a legally protected privacy interest, 2) a reasonable expectation of privacy in the circumstances, and 3) an intrusion so serious as to be an egregious breach of social norms.

In *Hernandez, v. Hillsides, Inc*., the California Supreme Court concluded that while a jury could find a surveillance video camera placed in the Plaintiffs' office an invasion of the employees' reasonable expectation of privacy, it was not severe enough to render the employee liable. *Hernandez, v. Hillsides, Inc*., 47 Cal. 4th 272 (2009). The court expressed that the defendants made "vigorous efforts to avoid intruding on plaintiffs' visual privacy altogether. Activation of the surveillance system was narrowly tailored in place, time, and scope, and was prompted by legitimate business concerns. Plaintiffs were not at risk of being monitored or recorded during regular work hours and were never actually caught on camera or videotape." *Id.* at 301.

Cal. Gov. Code §12940 – Includes sexual orientation, gender identity, and gender expression among the list of categories protected from employment discrimination.

Cal. Labor Code §432.7 – Prohibits public and private employers from asking an applicant to disclose information concerning an arrest or detention that did not result in a conviction, or information concerning a referral to and participation in any pretrial or post trial diversion program. Limitations also apply to: a

conviction for possession of 28.5 grams or less of marijuana, unless it is "concentrated cannabis."

COLORADO

Off-Duty Activity

Colorado makes it illegal for an employer to terminate an employee because that employee engaged in any lawful activity off the employer's premises during non-working hours, unless the restriction (1) relates to a bona fide occupational requirement or is reasonably and rationally related to the employment activities and responsibilities of a particular employee or a particular group of employees; or (2) is necessary to avoid, or avoid the appearance of, a conflict of interest with any of the employee's responsibilities to the employer. Colo. Rev. Stat. §24-34-402.5 (2005).

CONNECTICUT

Off-duty tobacco use

Connecticut by statute has limited the ability of both public sector and private sector employers to require employees or job applicants to refrain from off-duty use of tobacco products outside of the course of employment or otherwise to discriminate against either job applicants or current employees based on such off-duty use. There is an exemption, however, for nonprofit organizations whose primary purpose is to discourage use of tobacco products by the general public. *See* Conn. Gen. Stat. § 31-40q(a)(2); Conn. Gen. Stat. § 31-40s.

Electronic monitoring by employers

Employers who engage in any type of electronic monitoring must "give prior written notice to all employees who may be affected, informing them of the types of monitoring which may occur." Conn. Gen. Stat. § 31-48d(b)(1) (2008). The statute is enforced by the Connecticut Department of Labor. There does not appear to be a private right of action for employees to sue employers under the statute (see *Gerardi v. City of Bridgeport*, above).

Personal information collected by employers

In 2008, Connecticut passed a law (Public Act 08-167, effective October 1, 2008) which imposed new obligations on employers with respect to protecting various forms of personal information they may collect from people, including their own employees. As to Social Security numbers, companies are required to create a

"privacy protection policy" which, at minimum, must (1) protect the confidentiality of Social Security numbers, (2) prohibit unlawful disclosure of Social Security numbers, and (3) limit access to Social Security numbers. The privacy protection policy must be published or publicly displayed. The Act protects more than just Social Security numbers as the term "personal information" is broadly defined in the new statute to mean "information capable of being associated with a particular individual through one or more identifiers," which include items such as social security numbers, driver's license numbers, state identification card numbers, account numbers, credit or debit card numbers, passport numbers, alien registration numbers and health insurance identification numbers. Conn. Gen. Stat. § 42-471.

Identity theft and employment applications

In 2009, as part of a broader bill designed to combat identity theft, the legislature imposed a new obligation on employers with respect to employment applications. The new law imposed penalties on employers that fail to obtain and retain employment applications in a secure fashion, or who fail to take reasonable measures to destroy them or make them unreadable when disposing of them, at least by shredding them. 48 Pub. L. No. 09-239, An Act Concerning Consumer Privacy and Identity Theft.

DISTRICT OF COLUMBIA

Disclosure of personnel information

DC ST § 1-631.03 [Formerly § 1-632.3]. It is the policy of the District government to make personnel information in its possession or under its control available upon request to appropriate personnel and law-enforcement authorities, except if such disclosure would constitute an unwarranted invasion of personal privacy or is prohibited under law or rules and regulations issued pursuant thereto.

FLORIDA

Right to privacy

West's F.S.A. Const. Art. 1 § 23 - Right of privacy. Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein. This section shall not be construed to limit the public's right of access to public records and meetings as provided by law.

Employment records

The state constitutional privacy right may, under certain circumstances, extend to personal information contained in nonpublic employee personnel files. *Alterra Healthcare Corp. v. Estate of Shelley*, 827 So.2d 936 (2002).

Nursing home operator had standing to protect the right of privacy of its former employee by asserting that compelling production of employee's personnel file violated his right to privacy, in negligence suit brought by patient, who was injured in fall, against operator. *Beverly Enterprises-Florida, Inc. v. Deutsch*, App. 5 Dist., 765 So.2d 778 (2000), rehearing denied.

Public employment

In determining whether job applicant was entitled to protection under constitutional privacy provision, court would first determine whether government entity was intruding into aspect of applicant's life in which applicant had legitimate expectation of privacy, and, if it were to find in affirmative, would then look to whether compelling interest existed to justify that intrusion and, if so, whether least intrusive means was being used to accomplish the goal. *City of North Miami v. Kurtz*, 653 So.2d 1025 (1995), rehearing denied, certiorari denied 116 S. Ct. 701, 516 U.S. 1043.

GEORGIA

Wiretapping and eavesdropping

Ga. § 16-11-62 is a broad statute making it unlawful to eavesdrop, record, transmit or communicate "the private conversation of another."

Common law privacy standards

Georgia recognizes the four standard common law invasion of privacy claims: intrusion upon solitude or seclusion, public disclosure of private facts (e.g., unreasonable publicity given to one's private life), false-light privacy (e.g., publicity that normally places the other in a false light before the public), and appropriation of one's name or likeness. *Allen v. Atlas Cold Storage USA, Inc.*, 613 S.E. 2d 657 (Ga. App. Ct. 2005).

HAWAII

Right to privacy

Hawaii Const. Art. 1, § 6. The right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest. The legislature shall take affirmative steps to implement this right.

Hawaii Cons. Art. 1, § 7

Eavesdropping and wiretaps

Genuine issue of material fact as to whether pager carried by female police employee belonged to her or police department precluded summary judgment in employee's action against department for invading her privacy by tapping pager without warrant or permission. Hawaii Const. Art. 1, § 6. *Black v. City & County of Honolulu*, 112 F. Supp.2d 1041(2000).

Participant or consensual monitoring by government agent in face-to-face meeting with defendant in public park in which conversation was recorded on a tape recorder strapped to body of government agent did not violate constitutional right to privacy since no eavesdropping was involved where government agent was free to testify to what was heard and tape merely preserved her credibility. U.S.C.A. Const. Amend. 4; Const. Art. 1, § 6. *State v. Lester*, 1982, 64 Haw. 659, 649 P.2d 346, habeas corpus denied 751 F. Supp. 853, affirmed 934 F.2d 324, certiorari denied 112 S. Ct. 318.

Drug testing

Since fire department's suspicionless drug testing program by urinalysis was necessary means to compelling governmental interest, court was not required to decide whether drug testing might implicate right to privacy under State Constitution. Const. Art. 1, § 6. *Doe v. City and County of Honolulu*, 8 Haw. App. 571, 816 P.2d 306 (1991).

Police department's drug-testing program, required as a condition of employment, was the necessary means to a compelling state interest, and thus court need not decide whether compelled urinalysis testing might impede a right to privacy under the State Constitution. Const. Art. 1, § 6. *McCloskey v. Honolulu Police Dept.*, 71 Haw. 568, 799 P.2d 953 (1990).

Public employment

Information regarding police officer's misconduct in the course of his duties as police officer is not within the protection of Hawaii's constitutional right to

privacy. Const. Art. 1, § 6. *State of Hawaii Organization of Police Officers (SHOPO) v. Society of Professional Journalists-University of Hawaii Chapte*r, 83 Hawaii 378, 927 P.2d 386 (1996).

Information regarding charges of misconduct by police officers, in their capacities as such, that have been sustained after investigation and that have resulted in suspension or discharge is not "highly personal and intimate information" and, therefore, is not within the protection of Hawaii's constitutional right to privacy. Const. Art. 1, § 6. *State of Hawaii Organization of Police Officers (SHOPO) v. Society of Professional Journalists-University of Hawaii Chapte*r, 83 Hawaii 378, 927 P.2d 386 (1996).

Information that must be disclosed pursuant to Uniform Information Practices Act (UIPA) regarding public employee's employment related misconduct and resulting discipline is not "highly personal and intimate information" and, therefore, is not within scope of Hawaii's constitutional right to privacy. Const. Art. 1, § 6; HRS § 92F-14(b)(4)(B). *State of Hawaii Organization of Police Officers (SHOPO) v. Society of Professional Journalists-University of Hawaii Chapte*r, 83 Hawaii 378, 927 P.2d 386 (1996).

Financial disclosure requirements of county's ethics code did not violate State Constitution's privacy provisions where disclosure requirements paralleled those of Constitution's ethics provision, thus consistent with officials' reasonable expectations of privacy. Const. Art. 1, § 6; Art. 14. *Nakano v. Matayoshi*, , 68 Haw. 140, 706 P.2d 814 (1985).

ILLINOIS

Medical and genetic information

Illinois has the Genetic Information Privacy Act, as amended in 2009. 410 Ill. Comp. Stat. 513/1.

IOWA

Lie detector tests

An employer may not require an employee or applicant to take a lie detector test, nor can an employee be asked to sign a waiver to take the test. Iowa Code 8730.4

KENTUCKY

Smoking outside workplace protected

Kentucky prohibits private sector and public sector employers, other than the federal government, with eight or more employees from discriminating against an employee or job applicant because that individual is a smoker or a nonsmoker or from requiring that an employee refrain from smoking or using tobacco products outside the course of employment, as long as that individual complies with any workplace policy concerning smoking. It is not a violation of the law, however, for an employer to charge higher healthcare premiums to smokers. Ky. Rev. Stat. Ann. § 344.040.

MAINE

Tobacco use protected

Maine has enacted a statute that prohibits private sector employers from requiring as a condition of employment that an employee or prospective employee refrain from using tobacco products outside the scope of employment or from otherwise discriminating against an employee or job applicant based on use of tobacco products as long as the employee complies with any workplace policy concerning the use of tobacco. Me. Rev. Stat. Ann. tit. 26, § 597.

MASSACHUSETTS

Massachusetts Privacy Act

The Massachusetts Privacy Act, Mass. Gen. Laws c. 214, § 1B, which provides that:

A person shall have a right against unreasonable, substantial or serious interference with his privacy. The superior court [the state trial court] shall have jurisdiction in equity to enforce such right and in connection therewith to award damages.

The statute creates a private right of action for any aggrieved individual seeking equitable relief or damages. In determining whether there has been a violation of the statute, courts will balance the employer's legitimate business interest in an intrusion against the substantiality of the intrusion on the employee's reasonable expectation of privacy. In the employment context, the claims generally concern either (1) improper employer intrusion into purely private matters or (2) improper

employer publication (within or beyond the workplace) of private matters involving an employee.

Question as to employee whereabouts not invasion of privacy

Williams v. Brigham & Women's Hosp., Inc., 001546A, 2002 WL 532979 (Mass. Super. Jan. 8, 2002) (inquiry into employee's whereabouts by employer's security guard which caused employee to reveal that she had an abortion was not an unreasonable invasion of privacy where it was reasonably related to legitimate inquiry into employee's whereabouts in connection with investigation into check cashing scheme).

Urine sample shows nicotine use, not invasion of privacy

Rodrigues v. EG Sys., Inc., 639 F. Supp. 2d 131, 134 (D. Mass. 2009) (in keeping with employer's policy of not employing smokers, employee was terminated from employment with Scott's Lawn Service after urine sample showed nicotine use; no invasion of privacy where employee did not make secret of the fact that he was a smoker).

Release of records about employees who provided information to Attorney General

Pintado v. Nat'l Carpentry Contractors, Inc., 073898, 2009 WL 4282102 (Mass. Super. Nov. 6, 2009) (it would be an unwarranted invasion of privacy to release, in response to public records request, the names of employees who provided information to the Attorney General's Office concerning the alleged misclassification of workers).

MICHIGAN

Medical / Genetic information

Michigan has the Persons with Disabilities Civil Rights Act (Mich. Comp. Laws, §37.1101), which defines "genetic information" and "genetic test," and prohibits discrimination on the basis of genetic information. Employers cannot require employees or applicants to submit to a genetic test or to provide genetic information as a condition of employment or promotion.

MINNESOTA

Social Security number and identity privacy

Minnesota has a Social Security Privacy Act that was amended in 2008. Minn. Stat. § 325E.59, as amended by 2008 Minn. Laws 333.

Medical / Genetic information

Minnesota has the Genetic Testing in Employment statute which protects employees from being discriminated against based on genetic information. The law also prohibits employers from engaging in genetic testing and using test results as a condition of employment. Minn. Stat., Ch. 181, Sec. 974, as amended by Ch. 9, L. 2001.

Gender Identity and Sexual Orientation

Minnesota has a Human Rights Act which prohibits discrimination on the basis of a person's actual or perceived sexual, physical, or emotional attachment to another person without regard to the sex of that person. Employers, employment agencies, and unions cannot ask prospective employees or members about their sexual orientation. Minn. Stat. §363A.01, as amended by Ch. 215, L. 2008.

Use of lawful products

Minnesota law prohibits an employer from refusing to hire a job applicant or disciplining or discharging an employee for using lawful consumable products, if the products are used off the employer's premises outside of working hours and provides for an exception related to a bona fide occupational requirement that is reasonably related to the employment activities or responsibilities of a particular employee or group of employees or where it is necessary to avoid a conflict of interest or the appearance of a conflict of interest. Minn. Stat. Ann. §181.938 (2003).

Lie detector test

An employer may not directly or indirectly solicit or require an employee or applicant to take a lie detector test. Results of a voluntary test may be given only to those authorized by the employee. Minn. Stat. Ann. §181.75.

MISSOURI

Use of lawful products

An employee cannot refuse to hire, discipline or discharge based upon an employee's lawful use of tobacco or alcohol. Mo. Rev. Stat. §290.145 (2004).

NEBRASKA

Lie detector test

An employer cannot require an employee or prospective employee to submit to a polygraph examination or voice stress analysis unless they are employed as law enforcement officials. An employer may request that an employee take such a test if certain conditions are met. Any violation of the statute is a misdemeanor. Neb. Rev. Stat. § 81-1932.

NEVADA

Drug and alcohol testing results

N.R.S. 284.4068. State Personnel Alcohol and Drug Test Results are Confidential. Results must be securely maintained and separately kept from other files concerning personnel.

Exceptions to disclosure. Written consent of the person tested; Required by medical personnel for the diagnosis or treatment of the person tested if the person is physically unable to give the person's consent to disclosure; Properly issued subpoena; When relevant in a formal dispute between the appointing authority and the person tested; and As required for the administration of a plan of benefits for employees.

NEW HAMPSHIRE

Interception of off-duty call constituted invasion of privacy

Karch v. BayBank FSB, 147 N.H. 525 (2002) (plaintiff stated a claim for invasion of privacy against individuals who intercepted, via radio scanner, her private off-duty telephone conversation with a co-worker, during which some arguably negative remarks about employer were made, and then disclosed the content of those conversations to the employer, which resulted in the employer terminating the employee's employment).

Use of tobacco products outside course of employment

No employer shall require as a condition of employment that any employee or applicant for employment abstain from using tobacco products outside the course of employment, as long as the employee complies with any workplace policy, pursuant to RSA 155:51-53 and, when applicable, RSA 155:64-77.

NEW JERSEY

Interception of electronic and oral communications

New Jersey § 2A:156A-3 restricts the interception, disclosure and use of wire, electronic and oral communication, making it a crime of the third degree. The law does not apply to the contents of any wire, electronic or oral communication that has become "common knowledge or public information," which could be applicable in social networking situations.

Wiretapping law and electronic surveillance

The New Jersey Wiretapping and Electronic Surveillance Control Act ("NJ Wiretap Act"), N.J.S.A. 2A:156A-27, provides that: "A person is guilty of a crime of the fourth degree if he (1) knowingly accesses without authorization a facility through which an electronic communication service is provided or exceeds an authorization to access that facility, and (2) thereby obtains, alters, or prevents authorized access to a wire or electronic communication while that communication is in electronic storage." N.J.S.A. 2A:156A-27(a). "Electronic storage," as used in the NJ Wiretap Act, is defined as: "(1) Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (2) Any storage of such communication by an electronic communication service for purpose of backup protection of the communication." N.J.S.A. 2A:l56A-2(q).

NEW MEXICO

Sexual orientation and gender identity

§28-1-7. Effective January 1, 2007, sexual orientation and gender identity were added to the list of categories protected from employment discrimination. Employers may not discriminate against a prospective or current employee based on sexual orientation or gender identity.

NEW YORK

Lawful activities

Employees are protected from employer discrimination based on recreational activities, certain political activities, and the use of consumable products. Lawful activities are protected when conducted away from the work site, outside of work hours, and without using the employer's equipment. Personal relationships (i.e.,

romance) is not considered a protected recreational activity under the statute; thus, employer non-fraternization policies are enforceable. N.Y. Lab. Law § 201-d (1992)

No common law cause of action for invasion of privacy

New York does not recognize a common law cause of action for invasion of privacy. New York does, however, provide a statutory cause of action for commercial use of one's likeness without consent. N.Y. Civ. Rights Law §§ 50, 51 (2008).

NORTH DAKOTA

Use of lawful products or lawful activity

It is a discriminatory practice for an employer to fail or refuse to hire a person; to discharge an employee; or to treat a person or employee adversely or unequally with respect to application, hiring, training, apprenticeship, tenure, promotion, upgrading, compensation, layoff, or a term, privilege, or condition of employment, because of participation in lawful activity off the employer's premises during non-working hours which is not in direct conflict with the essential business-related interests of the employer. N.D. Cent. Code 14-02/4-03.

OKLAHOMA

Use of lawful products

An employee cannot be disciplined or discharged because of lawful use of tobacco products. Okla. Stat. Title 40, §500 (2004).

OREGON

Employee privacy

659A.030. Effective January 1, 2008 (Superseded 659.030), sexual orientation and gender identity were added to the list of categories protected from employment discrimination. Employers may not discriminate against a prospective or current employee based on sexual orientation or gender identity.

Testing for drugs and alcohol, lie detectors and genetics

O.R.S. § 659A.300 makes it an unlawful employment practice for any employer to subject, directly or indirectly, any employee or prospective employee to any

breathalyzer test, polygraph examination, psychological stress test, genetic test or brain-wave test.

Exceptions to the statute:

An employer can lawfully administer a breathalyzer test with an employee's consent. Additionally, "if the employer has reasonable grounds to believe that the individual is under the influence of intoxicating liquor, the employer may require, as a condition for employment or continuation of employment, the administration of a blood alcohol content test by a third party or a breathalyzer test. The employer shall not require the employee to pay the cost of administering any such test."

O.R.S. § 659A.300 "does not prohibit the administration of a genetic test to an individual if the individual or the individual's representative grants informed consent in the manner provided by ORS 192.535, and the genetic test is **administered solely to determine a bona fide occupational qualification."**

PENNSYLVANIA

Wiretapping and Electronic Surveillance Act, 18 Pa. Cons. Stat. § 5701 et seq.

With limited exceptions for law enforcement, persons in the business of electronic communications, and public or consensual disclosures, Pennsylvania makes it a felony for a person to (1) intentionally intercept or endeavor to intercept any wire, electronic or oral communication; (2) intentionally disclose or endeavor to disclose to others the contents of any such interception; or (3) to intentionally use or endeavors to use the contents of any such communication, if the person knows or has reason to know it was unlawfully intercepted.

RHODE ISLAND

Off-duty use of tobacco products

Rhode Island by statute limits the ability of private sector and public sector employers to take action based on an employee's or job applicant's off-duty use of tobacco products. R.I. Gen. Laws § 23-20.10-14

Medical marijuana use protected

Rhode Island's statute relating to medical marijuana provides that "[n]o . . . employer may refuse to . . . employ . . . or otherwise penalize a person solely for

his or her status as a cardholder" of a valid registry identification card. R.I. Gen. Laws § 21-28.6-4.

TEXAS

No privacy right in usage of employer-provided phone or work calendar

In *Oyoyo v. Baylor Health Network, Inc*., No. Civ. A. 3:99CV0569L, 2000 WL 655427 (N.D. Tex., May 17, 2000), the employer reviewed the employee's telephone records and monitored her phone calls, and copied her personal calendar from her office. The court rejected the employee's invasion of privacy claims, noting that (1) the company provided the phone to the employee for business purposes – not personal usage; (2) the employer had reasonable concerns about the employee's excessive, non-business use of the phone; and (3) the calendar had been posted on her office wall, defeating any contention that she intended it to be private.

VERMONT

Sexual orientation, gender identity and dress code

Vermont's anti-discrimination in the workplace law which makes it unlawful to discriminate on the basis of, *inter alia*, sexual orientation or gender identify, expressly provides that "Notwithstanding any provision of this subchapter, an employer shall not be prohibited from establishing and enforcing reasonable workplace policies to address matters related to employees' gender identity, including permitting an employer to establish a reasonable dress code for the workplace." Vt. Stat. Ann. tit. 21, § 495 (West)

WASHINGTON

State Constitution

Article 1, section 7 of the Washington Constitution states: "No person shall be disturbed in his private affairs, or his home invaded without authority of law."

Washington's Privacy Act, RCW 9.73.

The Privacy Act states, in pertinent part, that it is unlawful to record "any private communication transmitted by telephone . . . radio or other device between two or more individuals using any device . . . designed to record and/or transmit said

communication . . . without first obtaining the consent of all the participants in the communication."

A violation of RCW 9.73 creates a private right of action for damages and attorney fees, and evidence obtained in violation of the statute is inadmissible.

Protected groups include sexual orientation and veterans

Wash. Rev. Code Ann. § 49.60.180 includes sexual orientation and honorably discharged military veterans among the list of categories protected from employment discrimination.

Genetic tests

Wash. Rev. Code Ann. § 49.44.180 prohibits genetic testing. The statute states in pertinent part: "[i]t shall be unlawful for any person, firm, corporation, or the state of Washington, its political subdivisions, or municipal corporations to require, directly or indirectly, that any employee or prospective employee submit genetic information or submit to screening for genetic information as a condition of employment or continued employment.

Lie detector tests

Wash. Rev. Code Ann. § 49.44.120 significantly restricts an employer's use of lie detector testing and makes it unlawful for employers (other than law enforcement agencies, drug manufacturers and distributors, and security organizations) to require an employee or prospective employee to take a lie detector test or similar test as a condition of employment or continuing employment. The law permits employees required to submit to a polygraph or similar test to sue the employer for damages. However, if an employee consents to be tested, an employer may use the results of the test as the basis for disciplinary action.

Note: employers in the state of Washington must comply with both Washington law and the Federal Employee Polygraph Protection Act of 1988.

WYOMING

Use of lawful products

An employee cannot be disciplined or discharged for lawful use of tobacco products. Wyo. Stat. §27-9-105 (2004).