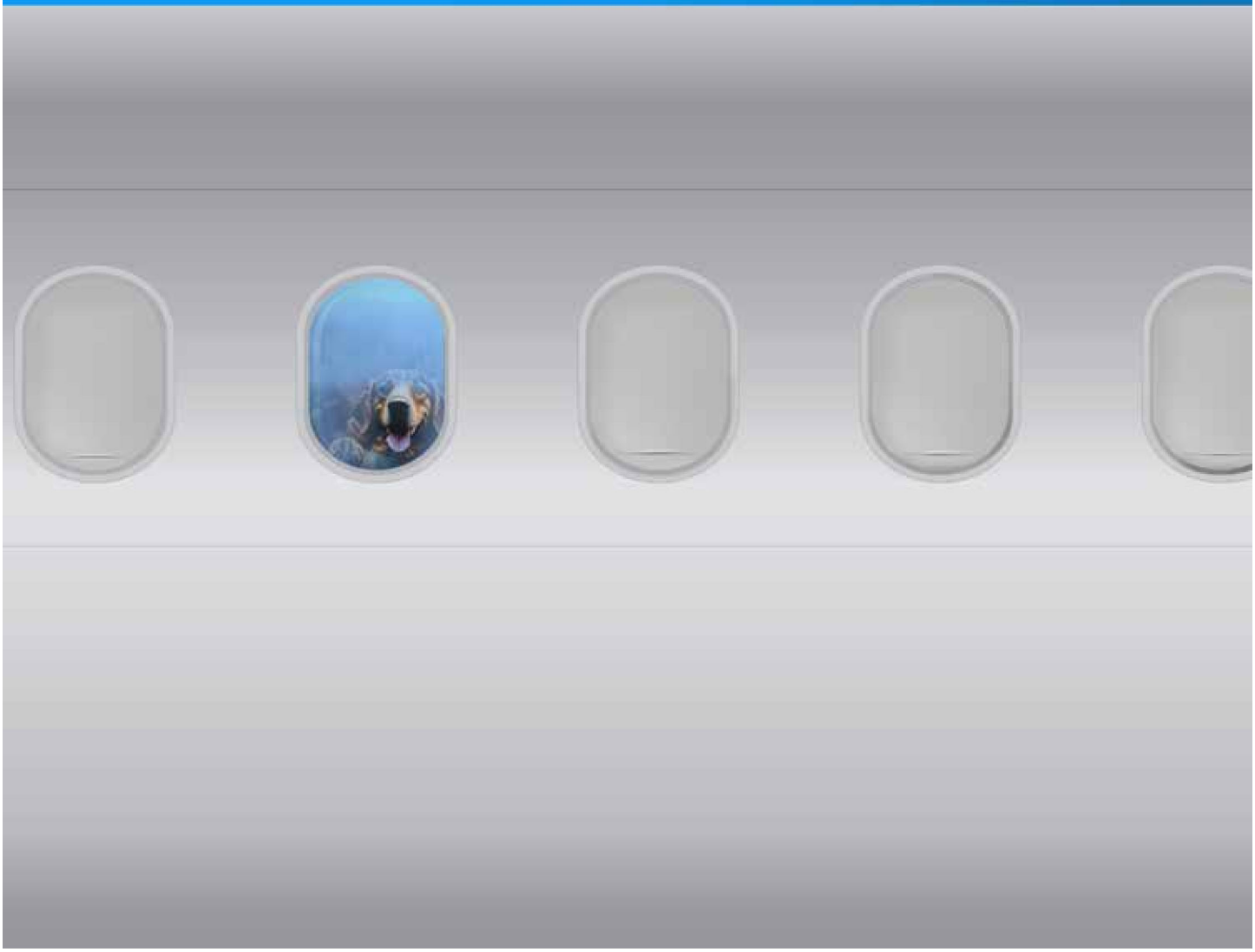
IMLA

Municipal Lawyer

THE JOURNAL OF LOCAL GOVERNMENT LAW

SEPT OCT
2023
VOL.64
NO.05

Flying With Fido: A Brief Survey of Federal Service Animal Law



OFFICERS
PRESIDENT
Lori Grigg Bluhm
City Attorney
Troy, Michigan
PRESIDENT ELECT
Rose Humway-Warmuth
City Solicitor
Wheeling, West Virginia
IMMEDIATE PAST PRESIDENT
Barbara A. Adams
General Counsel
Illinois Local Government Lawyers Association
TREASURER
Jeffrey Dana
City Solicitor
Providence, Rhode Island
GENERAL COUNSEL AND EXECUTIVE DIRECTOR
Amanda Karras
IMLA, Rockville, Maryland
BOARD OF DIRECTORS
Christopher Balch
City Attorney
Brookhaven, Georgia
Shauna Billingsley
City Attorney
Franklin, Tennessee
Alan Bojorquez
City Attorney
Bastrop, Texas
Beth Anne Childs
Town Attorney
Bristow, Oklahoma
Diana Cortes
City Solicitor
Philadelphia, Pennsylvania
Bradford Cunningham
Municipal Attorney
Lexington, South Carolina
Arthur Gutekunst
Sr. Assistant Corporation Counsel
White Plains, New York
Nina R. Hickson
City Attorney
Atlanta, Georgia
Lori Lein
General Counsel
Alabama League of Municipalities
Wynetta Massey
City Attorney
Colorado Springs, Colorado
Paige Mims
City Attorney
Plano, Texas
Kimberly Rehberg
City Attorney
Durham, North Carolina
Todd Sheeran
City Attorney
Herriman, Utah
Jennie Granahan Tarr
Chief Assistant County Attorney
Hillsborough County Hospital Authority
Nancy Thompson
City Counselor
Columbia, Missouri
Randall Van Vleck
Town Attorney
Kirtland, New Mexico
Wendy Walberg
City Solicitor
Toronto, Ontario
Byron Werry
City Solicitor
Regina, Saskatchewan
Jeannine Williams
Chief Assistant City Attorney
St. Petersburg, Florida
Susana Alcala Wood
City Attorney
Sacramento, California

CONTENTS

SEPTEMBER / OCTOBER 2023

FLYING WITH FIDO: A BRIEF SURVEY OF FEDERAL SERVICE ANIMAL LAW

By: Michelle Villareal, Deputy City Attorney, League City, Texas

Every year it seems that more of us are relying on the benefits of "emotional support" creatures, bringing them into previously animal-free environments. While these companions, four-legged or otherwise, undoubtedly provide great benefits, many are not "service animals" for purposes of federal law. Our author explains the regulations governing animals on airlines and related statutory nuances.

PAGE 6

THE PREROGATIVE TO UNSEAT: REMOVING COUNCILMEMBERS FROM COUNCIL COMMITTEES

By: Stephen K. Postema, City Attorney Ret., Ann Arbor, Michigan and Jennifer A. Richards, Assistant City Attorney, Ann Arbor, Michigan

Most city councilmembers comport themselves in a productive and cooperative manner. Occasionally, however, the city or county attorney will be called upon to evaluate the prospects for redressing unprofessional or unethical behavior by a councilmember. One such action may be to remove the member from a committee post. A thorough understanding of the rules and ramifications is required.

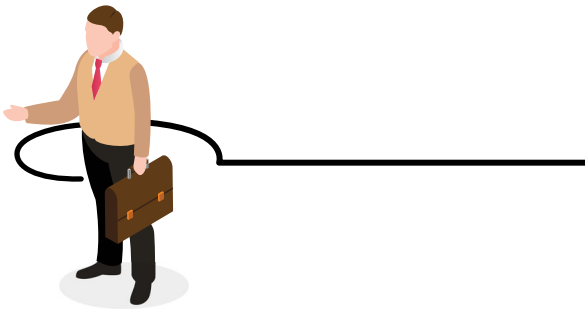
PAGE 10

"WE'RE HIRING, WE JUST NEED YOUR SOCIAL MEDIA LOGINS AND PASSWORDS"

By: Laura S. Burton, Police Attorney, Gastonia, North Carolina

Checking a job applicant's social media activity can provide a wealth of information, potentially revealing troublesome behavior and helping to avoid future problems. But such an inquiry triggers statutory and even constitutional issues, and many jurisdictions prohibit searching through a job seeker's non-public online activity.

PAGE 14



COVER AND FEATURE ILLUSTRATIONS BY TRUJILLODESIGN.NET

DEPARTMENTS

18 EMPLOYMENT
Marital Secrets: Spousal Privilege in Administrative Employment Proceedings
By: Nancy C. Rodgers, City and County Attorney, Broomfield, Colorado
When and where spousal secrecy can be maintained.

22 PRACTICE TIPS
City Attorneys: Things They Wish They Knew Before Running for Office
By: Karen L. Horner, City Attorney, Friendswood, Texas
Getting elected is just the beginning.

27 CITY PLANNING
Stub Streets: At the Corner of Essential Nexus and Rough Proportionality
By: Chase B. Ames, Assistant City Attorney, West Jordan, Utah
A dead-end street can have big legal consequences.

30 SUPREME COURT
Public Accommodations Law, Freedom of Speech, and Freedom of Religion
By: Megan Luptowski, Assistant City Attorney, Grand Rapids, Michigan
Expanding First Amendment protection of creative output.

34 INSIDE CANADA
Expanding Borders, Solicitor-Client Privilege, Roadway Spills, and More
By: Monica Ciriello, Director of Municipal Law and Licensing Compliance, City of Hamilton, Ontario
Recent cases of interest.

38 LISTSERV
The Parallel Universe
By: Brad Cunningham, Municipal Attorney, Lexington, South Carolina
Sovereign citizens on Main Street

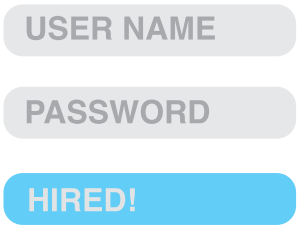
STAFF

EXECUTIVE EDITOR Amanda Karras
EDITOR Erich R. Eiselt
ART DIRECTION AND PRODUCTION Trujillo Design
MARKETING Caroline Storer

Views appearing in *Municipal Lawyer* are those of the authors. Publication of articles in this magazine does not reflect a direct or implied endorsement of an author's views. © Copyright 2023 by the International Municipal Lawyers Association (IMLA). All rights reserved. IMLA is a non-profit professional association of municipal lawyers from across the United States and Canada. It offers its members continuing legal education courses, research services, litigation assistance on amicus briefs and an information-sharing network in the field of municipal law. *Municipal Lawyer* is IMLA's membership magazine, published bi-monthly. For membership information contact: IMLA, 51 Monroe Street, Suite 404, Rockville, Maryland 20850, phone: (202) 466-5424, or e-mail: info@imla.org. Contributions of articles are welcome; email eeiselt@imla.org. *Municipal Lawyer* reserves the right to refuse or edit manuscripts submitted for publication.

"We're Hiring, We Just Need your Social Media Logins and Passwords"

By: LAURA S. BURTON,
Police Attorney, Gastonia, North Carolina



We all know that question—the one your client asks that causes you to cringe, frown and shake your head "no" before your client has even finished asking. That was my reaction when one of our recruiting sergeants asked me to review a form she had created that allows the city to ask law enforcement applicants for their logins and passwords for their social media accounts. No one is going to dispute the critical need to thoroughly evaluate a potential hire's background—for any government or private sector job. With law enforcement, the vetting of an applicant can be particularly important. But, combing through and investigating the non-public content of an applicant's social media? That just seems like it goes too far and is only going to open a can of worms even before considering any legal ramifications.

1. The Prevalence of Social Media Checks. I was surprised to learn in my home state of North Carolina that it is not outlawed by statute, despite attempts in prior legislative sessions to make it unlawful. At least one law enforcement agency in North Carolina, as a condition of employment, requires an applicant's social media information and mandates that the applicant provide access in the presence of a background investigator. The applicant signs a form that states that they understand that any information that is considered racist, sexist, or could bring discredit upon his or her candidacy for employment could disqualify him or her from further consideration with the agency. Another North Carolina agency, as part of its application procedure, has an applicant fill out a document listing each social media account he or she maintains or had in the past with a note that it is very important for the agency to be able to conduct a thorough background check as part of the hiring process. A Florida agency does not require passwords, but has an applicant sign a document listing any social media sites the applicant believes has content he or she posted and agrees to log on to those sites in the presence of a background investigator. According to the Florida agency's form, failure to disclose a site or not allowing an investigator to research the account may result in removal from the hiring process. A Georgia transit authority is similar—it mandates that sworn and non-sworn applicants for hire identify their social media accounts for the last three years and indicates that they will likely have to log on to their social media accounts in the presence of a background investigator.

Employment background checks are not new. They date back at least 100 years. They came to exist as negligent hiring and other legal claims developed when injured parties sought recourse from employers. The extent of a background check for a prospective employee varies greatly by sector and industry. With law enforcement officers at any level, it is often mandated by law and is intrusive. The federal government performs background checks on all permanent employees, the extent of which varies by position.[1] Most positions in finance, banking and healthcare are the same.

2. Risks of Litigation. Litigation surrounding background checks is also not new. After the federal government changed its policy, mandating that its contractor employees be subjected to a complete background check, the National Aeronautics and Space Administration (NASA) was challenged by those contractors. The government contractors argued that NASA's background check process violated a constitutional right to informational privacy.[2] The Supreme Court, in assuming a constitutional privacy interest was implicated, concluded that the federal government's questions were reasonable in light of the government interests at stake.[3] The Court noted that the federal government has had mandatory background checks in place for its federal civil-service applicants since 1953 and that any further disclosure of such personal information discovered in the background checks was shielded by federal statute.[4]

Unquestionably, there are many well-grounded reasons to conduct background checks—protecting an employer's reputation, ensuring the safety of the public and your workforce, endeavoring to predict reliability and dependability in an applicant, and attempting to minimize theft and other fraudulent or criminal activities are just a few reasons.[5] But, does a background check inquiring into an applicant's non-public social media cross the line? In *In re Ramirez,* an employer considered petitioner's discriminatory remarks on an old social media account when it chose to remove him from a 2020 eligibility list for police officers.[6] Two years earlier he had applied for the police department and at that time maintained the social media account.[7] He was removed from the eligibility list in 2018 as well.[8] In an administrative appeal, the Commission found that his racial and sexual comments evinced the lack of good judgment required for municipal law enforcement officers.[9] The opinion does not clarify whether the social media posts were public or non-public. Nonetheless, presumably, an employer would prefer not to hire a law enforcement officer who could be racist or sexist and who could increase its legal exposure.

3. Prohibitions Against Requiring Disclosure.

Currently, twenty-six states have laws specifically prohibiting an employer from requesting or requiring that an employee or applicant disclose login and password information or from otherwise gaining access to or viewing their non-public personal internet or social media accounts.[10] Some prohibit an employer from requiring an employee or applicant from divulging or disclosing any content from a social media account. There is no federal law specifically prohibiting employers from seeking login and password information of employees or prospective employees.[11] Despite general parallels as to what is off-limits to an employer, some statutes vary in what encompasses social media or a protected personal internet account and what is actually prohibited by an employer.[12] There are also significant variations among the states' exceptions to the prohibitions, meaning the instances when the employer can access the non-public personal account information. Almost every statute expressly permits employers to use what is publicly available about an employee or an applicant.[13] Most, if not all of these statutory schemes prohibit employers from using usernames and passwords if they were inadvertently acquired. Some of these workplace privacy statutory schemes apply to educational institutions and landlords.[14]

Maryland was the first state to make effective the Password Privacy Protection Act—prohibiting an employer from requesting or requiring that an employee or applicant disclose any user name and password or other means to access a personal account or service.[15] "Personal account" or "service" is not defined. Wisconsin passed a similar law two years later.[16] Wisconsin's statute applies to the state and its political subdivisions including local governments, and prohibits employers from requesting or requiring an employee or applicant, as a condition of employment, to disclose access information for their respective personal internet account or otherwise give the employer access to or allow observation of that account.[17] Personal internet account means an internet-based account created and used by an individual exclusively for purposes of personal communications,[18] suggesting that if an internet based account, such as a Facebook account, is used in any way for work-related communications, it is no longer restricted. Unlike other states, it is permissible in Wisconsin for an employer to require an employee, but not an applicant, to disclose a personal e-mail address, but not its password.[19] California defines social media as an electronic service or account or electronic content such as videos, still photographs, blogs, podcasts, instant and text messages, email, online services or accounts, or internet web site profiles.[20] Connecticut's definition of personal online account includes retail-based internet web sites, a broader definition than seen in most states, but also states that it is an account used exclusively for personal purposes. It includes electronic mail.[21] Colorado uses the term "personal account" and Washington uses the phrase "personal social networking account" but neither define it.[22] Illinois, on the other hand, states that a personal online account is one that is used by a person primarily for personal purposes.[23]

4. Loopholes in Prohibition.

From the first enacted statutes as noted above, the majority of states prohibit the employer from requesting or requiring an applicant or employee to share their social media usernames and passwords[24] and prohibit requiring that an applicant or employee access their social media accounts in the presence of the employer so the employer can observe same.[25] Other access "loopholes", however, needed to be closed. Later legislative social media privacy statutes included language prohibiting employers from mandating that an employee or applicant add the employer to his or her list of contacts or coercing an employee or applicant to change their settings for greater access to third parties.[26] Rhode Island prohibits requiring or coercing an employee or applicant from divulging any social media account information.[27] Maine, similarly, states that an employer may not require or coerce an employee or applicant to disclose any personal social media account information.[28] Montana further restricts an employer from requiring or requesting an employee or applicant to divulge any personal social media or information contained on personal social media.[29] Vermont states that an employer shall not require an employee or applicant to divulge or present any content from the respective social media account.[30] These provisions seem to place a prohibition on questions during an interview of an applicant such as "what social media accounts do you maintain," and "what would your social media tell us about you?" Although Hawaii prohibits an employer from requiring, coercing or requesting an employee to disclose the

Continued on page 16



Laura Burton has been the Police Attorney for the City of Gastonia, North Carolina, since late 2016. She advises the City on police and non-police matters. She began her municipal attorney career in 2004 at the City of Atlanta as an Associate Attorney, years later becoming its Deputy City Attorney for Litigation and Employment before departing for North Carolina. Ms. Burton received her law degree, with high honors, from the University of Florida, Levin College of Law.. She also received her undergraduate degree from Florida. She is a certified Guardian ad Litem in North Carolina. Laura also provides volunteer legal services to Best Friends Animal Society.

content of the protected personal online account, it surprisingly allows an employer to request that an employee add the employer to the set of persons to which the employee grants access to the content of the account if it is done without coercion and pursuant to a clear statement that acceptance is voluntary.[31]

Paralleling a common exception found in many statutes, Wisconsin employers can require an employee to grant access or allow observation of his or her social media account in conjunction with certain workplace investigations, but an employer cannot obtain the access information for those accounts.[32] These workplace investigations include inquiries into any alleged unauthorized transfer of the employer's proprietary or confidential information to the employee's personal internet account or any other alleged employment related misconduct, including violations of law, when the employer has reasonable cause to believe that activity on the personal internet account is related to that misconduct.[33] Tennessee mandates that an employee cooperate in an investigation but only requires the employee to share content in order to make a factual determination.[34] The employer must have specific information about the employee's unauthorized transfer of proprietary or confidential information or otherwise must have knowledge of specific information on the employee's personal internet account regarding compliance with laws or workplace rules.[35] Utah's provision is virtually identical.[36] West Virginia's statute does not have a specific information prerequisite before the employer can ask an employee to share content related to compliance with laws, regulations or other work place conduct rules.[37] Rhode Island provides an exception to employers allowing them to require or coerce an applicant or employee to divulge personal social media account information when it is reasonably believed to be relevant to a misconduct investigation. That information can be used to access social media to the extent necessary for the investigation.[38] On the other end of the spectrum, Montana allows an employer to demand user names and passwords to access social media when "an investigation" is under way and the information requested of the employee is necessary to make a factual determination in the investigation.[39]

Also a common exception, Wisconsin allows an employer to mandate access information if it is needed to gain access to or to operate an electronic communication device supplied or paid for by the employer or to gain access to an account or service provided by the employer.[40] Maine permits employers to promulgate polices that include a requirement that an employee disclose a user name or password or other necessary information to access employer-issued electronic devices or to access employer provided software or e-mail accounts.[41] Oklahoma ensures that employers are able to access their own computer system or information technology networks.[42] Oklahoma has a particularly noteworthy section in its statute about employer access to its own computer system and own electronic communication devices—Oklahoma's statute states "neither this section nor any other Oklahoma law shall prohibit an employer from *reviewing or accessing* personal online social media accounts that an employee *may choose to use while utilizing an employer's computer system, information technology network or an employer's electronic communication device*." At any point during the workday then, if an employee checks a personal social media account on a work computer or work phone, which, in Oklahoma, includes an employee's personal email account, Oklahoma employers are not prohibited from reviewing or accessing those accounts.[43]

5. Compliance with Law.

Many of the statutes include provisions that expressly state that the prohibitions from acquiring access to non-public personal internet account information do not prohibit employers from engaging in things required of them by law—some allowing access to social media content and some not. For example, Wisconsin's statute states that an employer is not prohibited from "complying with a duty to screen applicants for employment prior to hiring or a duty to monitor or retain employee communications that is established under state or federal laws, rules, or regulations or the rules of a self-regulatory organization, as defined in 15 U.S.C. 78c(a)(26)."[44] Wisconsin makes no reference here, however, to being able to access user names and passwords, unlike its section on workplace investigations. Nebraska is the same as Wisconsin.[45] Louisiana's statute is similar. It explains that an employer is not prohibited from complying with a duty to screen employees or applicants prior to hire or to monitor or retain employee communications pursuant to state or federal law, rules or regulations, case law, or rules of self-regulatory organizations, but makes no reference to accessing user names and passwords or obtaining specific social media content.[46] If complying with its legal and regulatory obligations, Vermont employers can request that an employee share specifically identified content.[47] West Virginia employers can request that an employee share specific content to ensure compliance with applicable laws or regulatory requirements.[48] Meanwhile, Montana employers can obtain user names and passwords to access personal social media when the employer is required to ensure compliance with federal laws or federal regulatory requirements or with the rules of self-regulatory organizations.[49]

6. Policies Specific to Law Enforcement.

Notably, Colorado, Connecticut and New Jersey specifically exclude law enforcement agencies from the definition of "employer" in their workplace privacy statutes.[50] New Mexico's law states that it does not apply to federal, state and local law enforcement agencies.[51] Colorado and New Jersey go even further and exclude the department of corrections and county corrections' departments, giving these employers the opportunity to search the private social media platforms of their applicants and employees.[52] Oregon's workplace privacy statute states that it does not apply to law enforcement units as defined by state law.[53] Connecticut only excludes state or municipal law enforcement agencies when conducting a pre-employment investigation of law enforcement personnel, thereby limiting permissible access to personal online accounts to the pre-employment hiring context.[54] Instead of excluding law enforcement from the definition of employer, Vermont specifically permits law enforcement agencies to require or request that an applicant provide access to his or her social media account as part of a screening for fitness during the hiring process.[55] Vermont law enforcement agencies can require the same of employees if in relation to a continued fitness determination or an investigation of employee misconduct.[56] None of these states seem to distinguish between sworn and non-sworn personnel. Washington actually requires that its background check for peace and corrections officers include a review of the applicant's social media account.[57] By stat-

ute, a peace officer or a correction officer must consent and facilitate the review of his or her social media account.[57] The employer is not allowed to obtain the login information.[59]

7. Constitutional and Statutory Protections.

Finally, many statutes contain specific provisions barring an employer from discharging, failing to hire, disciplining, threatening to discharge or discipline or otherwise retaliating or discriminating against an employee or applicant if they exercise their rights under these laws.[60] New Jersey and Nebraska further prohibit an agreement to waive those rights, expressing that it would be against public policy.[61] Vermont prohibits an agreement to waive without reference to public policy.[62] Oregon makes it an unlawful employment practice for an employer to require an employee or applicant to establish or maintain a personal social media account, a prohibition not seen in other states' statutes.[63] Montana has added a new subsection, effective October 2023, that prohibits an employer from discharging, disciplining or otherwise retaliating against an employee or job applicant for "legal expressions of free speech by the employee or job applicant, as protected in [Minnesota statute] 39-2-904, made on personal social media" in its workplace privacy law. Two exceptions apply; if the employee or applicant violates an employer's written policy or violates the terms or conditions of the employee's employment contract.[64]

Although there is no federal statute expressly prohibiting employers from requiring login credentials to peruse applicant and employees' social media accounts, prospective employees have sued employers alleging they violated federal employment anti-discrimination laws by using information gathered from internet and public social media searches in their hiring decision. In *Gaskell v. Univ. of Kentucky*, an applicant for a director position at the university observatory sued the school through Title VII[65] contending that he did not get selected because of his religious beliefs.[66] His religious beliefs were discovered when a hiring committee member conducted an internet search of him and discovered his personal web page that contained an article referencing religious topics combined with scientific theory.[67] The article was circulated to the search committee. In *Nieman v. Grange Mut. Cas. Co.*, a plaintiff successfully pleaded an Age Discrimination in Employment Act[76] (ADEA) claim and contended that the defendants were aware of his age through his LinkedIn profile and did not hire him.[69]

For the states that do not prohibit obtaining user names and passwords, these same federal employment laws (and likely many state laws) would apply to how information is used from employers' searches of employee or prospective employee's non-public social media in hiring decisions or other employment actions. Undeniably, various implicit biases, if factored into an employment decision, could violate Title VII, the ADEA, or the Americans with Disabilities Act.[70] Medical information, religious affiliation or disabilities could be discovered that an employer should not be privy to. We will inevitably see more lawsuits like *Gaskell* or *Nieman* and eventually the parameters of a constitutional right to informational privacy may be defined.

Conclusion

It seems a lot simpler if the employer does not review non-public social media content. These types of searches could require significant resources. How is the employer going to train its background investigators to evaluate the non-public social media content of prospective employees? Consistency will be critical as hiring decisions should be based on skills and qualifications for the positions, yet many lifestyle choices or conduct unrelated to skills and qualifications would be discovered. Moreover, is it just once that an employer would review the social media accounts or does it become an ongoing employment practice to monitor all employees' accounts? Although allowed in many states, accessing an employee or applicant's non-public social media seems precarious. For the time being at my North Carolina agency, there will be no review and no evaluation of an applicant's non-public social media content, preserving what is left, if anything, of the work-life home-life divide.

Notes

1. https://governmentworkerfi.com/background-checks-for-federal-employees/
2. NASA v. Nelson, 562 U.S. 134, 131 S. Ct. 746 (2011).
3. *See id.*
4. *See id.*
5. *See id.*
6. In re Ramirez, 2022 N.J. Super. Unpub. LEXIS 1857 (2022).
7. *See id.* at *2-3.
8. *See id.* at *2-3.
9. *See id.* at *7.
10. For example, Neb. Code Ann. §48-3503, 40 Okl. Stat. Ann. tit. 40, §173.2 and Cal. Lab. Code. §980. New Mexico's law only applies to prospective employees. N.M. Stat. §50-4-34.
11. The Stored Communications Act and the Computer Fraud and Abuse Act have proven unworkable in protecting employees and applicants from employers seeking access to their non-public social media or personal internet accounts. Carter, Ralph, Note and Comment, *Too Much Information!: The Need For Stronger Privacy Protection For the Online Activities of Employees and Applicants*, 28 J. Civ. Rts. & Econ. Dev. 291, 299-305 (2016).
12. As of September 2022, the states included: Arkansas, California, Colorado, Connecticut, Delaware, Hawaii, Illinois, Louisiana, Maine, Maryland, Michigan, Montana, Nebraska, Nevada, New Jersey, New Mexico, Oklahoma, Oregon, Rhode Island, Tennessee, Utah, Vermont, Virginia, Washington, West Virginia, and Wisconsin.
13. *See for example* Wis. Stat. §995.55(2)(b)(6). Montana's workplace privacy law does not include specific language permitting an employer to use what is publicly available regarding an applicant.
14. Wis. Stat. §995.55(3) and (4). Michigan's Internet Privacy Protection Act, one of the forerunners of this kind of legislation, also applies to educational institutions. Mich. Comp. Laws §37.274. Delaware has a section that applies to academic institutions and Rhode Island includes unlawful practices for educational institutions. Del. Code Ann. tit.14, §8103 and R.I. Gen. Laws §16-103.1 *et seq*. Louisiana also has a section that applies to educational institutions, La. Rev. Stat. Ann. §51:1954, as does Hawaii. Haw. Rev. Stat.§487G-4.
15. Md. Code Ann. Lab & Empl. §3-712. The effective date was October 1, 2012.
16. Wis. Stat. §995.55 (2013) (amended 2017).
17. Wis. Stat. §995.55(2)(a)(1)(2) and (3).
18. Wis. Stat. 995.55(1)(d). New Jersey also contains this exclusivity language. N.J. Stat. Ann. §34:6B-5.
19. Wis. Stat. §995.55(2)(b)(7). Louisiana does not prohibit an employer from requiring an employee to provide a personal email address, but only to facilitate communica-

Continued on page 21

Evidence § 505.09 (2d ed. 2016).
27. *Wolfle*, 291 U.S. at 12.
28. *Id.*
29. *Id.* at 14.
30. *Lavin*, 111 F.3d at 925.
31. e.g. Mich. Comp. Law, § 600.2162; Or. Rev. Stat. § 40.255; Fla. Sta. § 90.504; Va. Code Ann. § 8.01-398 (2005) (civil) and § 19.3-271.2 (2020) (criminal)
32. State v, Guttierez, 142 N.M. 1 (2007).
33. N.D.R. Evid. 504
34. Colo. Rev. Stat. § 13-90-107 (2023).
35. *Id.* at (a)(I).
36. Obergefell v. Hodges, 135 S. Ct. 2584 (2015); *See* In re Hogsett, 478 P.3d 713 (refining test for establishing common law marriage first articulated in *People v. Lucero* to reflect changed circumstances since that decision, including the recognition of same-sex marriage); In re LaFleur, 479 P.3d 869 (recognizing same-sex common law marriages predating Colorado's recognition of formal same-sex marriages).
37 Colo. Rev. Stat. § 13-90-107 (2023).
38. *Id.*
39. *Id.*
40. *Id.* at (a)(II).
41. *Id.*
42. *Id.* at 14.
43. *Lavin*, 111 F.3d at 925.
44. In re Witness Before Grand Jury, 791 F.2d 234, 237 (2d Cir. 1986) (quoting *Trammel*, 445 U.S. at 51) (internal quotations omitted).
45. *Blau*, 340 U.S. at 333.
46. Colo. Rev. Stat. § 13-90-107 (2023) (reference Article 90 (Court and Court Procedures) and Title 13 ("Witnesses"))
47. Riverside Cnty. Sheriff's Dep't v. Zigman, 169 Cal. App. 4th 763 (Cal. Ct. App. 2008).

We're Hiring *cont'd from page 17*

tion if the employer's email system fails. La. Rev. Stat. §51:1953(F).
20. Cal. Lab. Code §980(a).
21. Conn. Gen. Stat. §31-40x(a)(5).
22. Colo. Rev. Stat. §8-2-127; Wash. Code. Ann. §49.44.200. West Virginia also uses "personal account" and it means an account, service or profile on a social networking website that is used by an employee or potential employee exclusively for personal communications unrelated to any business purposes of the employer. W. Va. Code §21-5H-1.
23. 820 Ill. Comp. Stat. 55/10(b)(6)(B).
24. Md. Code Ann. Lab & Empl. §3-712.
25. Mich. Comp. Laws Serv. §37.273(a), effective December 28, 2012.
26. As examples: Or. Rev. Stat. §659A.330(1)(c), effective January 1, 2014; Del. Code Ann. tit. 19, §709A(b)(5) and (6), effective August 7, 2015; Neb. Rev. Stat. §48-3503, effective July 21, 2016; Vt. Stat. Ann tit. 21, §495l(b)(4) and (c), effective January 1, 2018.
27. R.I. Gen. Laws §28-56-2(3).
28. Me. Rev. Stat. Ann. tit. 26, §616(3).
29. Mont. Code. Ann. §39-2-307(1)(c).
30. Vt. Stat. Ann tit. 21, §495l(b)(3).
31. Haw. Rev. Stat. §487G-3(a)(1)(B).
32. Wis. Stat. §995.55(2)(b)(3). Virginia merely allows an employer to *request* the username and password for an investigation if the employer reasonably believes the employee's social media account information is relevant. Va. Code. Ann. §40.1-28.7:5(F)(2) (emphasis added).
33. Wis. Stat. §995.55(2)(b)(3).
34. Tenn. Code Ann. §50-1-1003(c).
35. Tenn. Code Ann. §50-1-1003(b)(3)(A) and (B).
36. Utah Code Ann. §34-48-201(2).
37. W. Va. Code Ann. §21-5H-1(b)(6). W. Va. Code Ann. §21-5H-1(b)(4) states that an employer can require an employee to cooperate in an investigation.
38. R.I. Gen. Laws §28-56-2(3).
39. Mont. Code Ann. §39-2-307(2)(b).
40. Wis. Stat. §995.55(2)(b)(1). Additional examples: Del. Code Ann. tit. 19, §709A(d) and Tenn. Code Ann. §50-1-1003(b)(1).
41. Me. Rev. Stat. Ann. tit. 26, §618.
42. Okla. Stat. Ann. tit. 40, §173.2 (F).
43. Okla. Stat. Ann. tit. 40 §173.2 (F) and (H)(2) (emphasis added).
44. Wis. Stat. §995.55(2)(b)(5).
45. Neb. Rev. Stat. §48-3507(8).
46. La. Rev. Stat. Ann. §51:1953(D). Virginia is similar, stating that an employer is not prevented from complying with the requirements of federal, state, or local laws, rules, or regulations or the rules or regulations of self-regulatory organizations. Va. Code. Ann. §40.1-28.7:5(F).
47. Vt. Stat. Ann. tit. 21, §495l(e)(1)(A).
48. W. Va. Code. §21-5H-1(b)(6).
49. Mont. Code. Ann. §39-2-307(2)(a)(iii).
50. Colo. Rev. Stat. §8-2-127(1)(c) and Conn. Gen. Stat. §31-40x(a)(3).
51. N.M. Stat. Ann. §50-4-34(D).
52. Colo. Rev. Stat. §8-2-127(1)(c); N.J. Stat. Ann. §34:6B-5 and §34:6B-6. New Jersey also excludes the State Parole Board.
53. Or. Rev. Stat. §659A.330.
54. Conn. Gen. Stat. §31-40x(a)(3).
55. Vt. Stat. Ann. tit. 21, §495l(e)(2).
56. Vt. Stat. Ann. tit. 21, §495l(e)(2).
57. Wash. Rev. Code Ann. §43.101.095(2)(b)(iv).
58. Wash. Rev. Code Ann. §43.101.095(4).
59. Wash. Rev. Code Ann. §49.44.200(3)(e).
60. Wisconsin prohibits an employer from discharging or otherwise discriminating against an employee for exercising their rights under the law and prohibits an employer from refusing to hire an applicant because the applicant refused to disclose access information, grant access or allow observation of the account. Wis. Stat. §995.55(2)(a) (2) and (3). *See for further example* 820 Ill. Comp. Stat. Ann. 55/10(b)(E) and (F) and Me. Rev. Stat. Ann. tit. 26 §616.
61. N.J. Stat. Ann. §34:6B-7; Neb. Rev. Stat. Ann. §48-3504. New Mexico contains neither provision. N.M. Stat. Ann. §50-4-34.
62. Vt. Stat. Ann. tit. 21, §495l(d).
63. Or. Rev. Stat. §659A.330(1)(a). Oregon also prohibits an employer from requiring an employee or applicant to allow the employer to advertise on their social media account. Or. Rev. Stat. §659A.330(1)(b).
64. Mont. Code Ann. §39-02-307(4)(b) and (5).
65.Title VII of the Civil Rights Act of 1964 prohibits employers from failing or refusing to hire or discharging any individual, or otherwise discriminating against any individual with respect to his compensation, terms, conditions, or privileges of employment, because of such individual's race, color, religion, sex, or national origin. 42 U.S.C. §2000e-2(a)(1).
66. Gaskell v. Univ. of Kentucky, 2010 U.S. Dist. LEXIS 124572 (E.D. Ky. 2010).
67. *See id.* at *10.
68. The Age Discrimination in Employment Act of 1967 prohibits age discrimination in employment. 29 U.S.C. §623.
69. Nieman v. Grange Mut. Cas. Co., 2012 U.S. Dist. LEXIS 59180, *4 (C.D. Ill. 2012).
70. The Americans with Disabilities Act of 1990 prohibits discrimination against individuals with disabilities in daily life. 42 U.S.C. §12101 *et seq.*