



Social Media: Legal Issues

Dear Reader:

The following document was created from the MTAS website ([mtas.tennessee.edu](https://www.mtas.tennessee.edu)). This website is maintained daily by MTAS staff and seeks to represent the most current information regarding issues relative to Tennessee municipal government.

We hope this information will be useful to you; reference to it will assist you with many of the questions that will arise in your tenure with municipal government. However, the *Tennessee Code Annotated* and other relevant laws or regulations should always be consulted before any action is taken based upon the contents of this document.

Please feel free to contact us if you have questions or comments regarding this information or any other MTAS website material.

Sincerely,

The University of Tennessee
Municipal Technical Advisory Service
1610 University Avenue
Knoxville, TN 37921-6741
865-974-0411 phone
865-974-0423 fax
www.mtas.tennessee.edu

Table of Contents

Social Media: Legal Issues	3
Social Media: Fair Credit Reporting Act	3
Social Media: Discrimination	3
Social Media: Disparate Impact	4
Social Media: Disparate Treatment	4
Social Media: Federal Employment Laws	5
Social Media: Invasion of Privacy	5
Social Media: Off-Duty Behavior	6
Social Media: Disciplining Employee for Online Activity	6

Social Media: Legal Issues

Reference Number: MTAS-1609

Inaccuracies and Context

Employers should exercise caution when looking for information about a person online. Some of what is posted online is not controlled by the applicant or the employee. Additionally, there is always the possibility you are not looking at the correct person's profile or that someone is impersonating an individual. A joke or comment posted on someone's profile by a "friend" in bad taste may not accurately reflect the character of your candidate or employee. A remark taken out of context may appear much more severe than its intent. Most users protect themselves by setting their privacy settings so that their profile is not open to the public. While privacy settings are meant to protect a user's personal information, the settings do not protect applicants and employees against fraud, impersonation, harassment, photo tagging, and photo editing. Employers must develop social media hiring policies that outline exactly how social media will be used in the hiring process. This information should be provided to candidates upfront and before an application is submitted. *Again, employers should use a trained human resources professional to screen candidates based on social media policy. Only job related information should be forwarded to the hiring manager.*

The following topics in this section include more details regarding social media legal issues.

Social Media: Fair Credit Reporting Act

Reference Number: MTAS-1610

An applicant may claim to have legal causes of action if he or she has been turned down for a job as a result of online information. Pursuant to certain provisions of the Fair Credit Reporting Act (hereinafter "FCRA"), an invasion of privacy lawsuit could be established and some experts suggest social networking sites themselves may be vulnerable to lawsuits under the FCRA. Employers should provide a written notice that explains your city may obtain a consumer report for employment purposes. Employers are also required by the FCRA to obtain the applicant's signature before performing a background check and releasing the information. This signature should be on a stand-alone FCRA notice and acknowledgement. A job application is not considered sufficient notice under the FCRA. If an adverse employment decision is made based on information discovered through a background check, the applicant should be notified as described in FCRA regulations.

Social Media: Discrimination

Reference Number: MTAS-1611

Discrimination Based on Protected Classes

Most social networking sites show an employer a person's gender or gender identity, race, age, sexual orientation, neighborhood, family members, religious views (or absence thereof), family status, pregnancy status, and political views. In some cases a person's profile may yield direct or indirect information about medical information, genetic issues, and health status. If potential employers have access to this information, how can they guarantee they will not use any of this information to make hiring or employment decisions? Once the information is viewed, there is no way to go back and undo what the employer has learned. This is perhaps, the largest employment risk associated with reviewing online profiles on candidates.

Potential liability arises when an employer uses the information found via social media to affect hiring and or employment decisions. For example, an employer is getting ready to make Sarah an offer, and suddenly finds Sarah's online profile and clearly sees she is pregnant. The employer may change the hiring decision based on the online information, which is illegal. In addition, the employer may have been able to determine Sarah's relative age, marital status, race and even religious and political affiliation. Employers making employment decisions based on information related to protected classes may be a violation of state, local, and federal laws.

Conversely, if the employer makes a poor hiring decision, the city could be accused of being negligent for failing to properly conduct background and pre-employment screening. With court dockets and other public information online, information on potential candidates is easier to obtain. For this reason, every city should have a policy on social networking and its use in the hiring process. Additionally, you should include in your policy if and when social media will be used in background checks and employee discipline and harassment investigations.

Discrimination laws prohibit employers from seeking out information that would disclose protected status information. If you will not ask a candidate if she/he has children in an interview, then it is not relevant to your online search either. Those with hiring or firing authority should be careful in accessing any profile that could reveal age, gender, relationship status, national origin, disability status, pregnancy status, health status etc. Employers should be following their social media policies and only consider legitimate job related information when hiring or making a decision that will impact someone's livelihood. Employers should always have a trained human resources professional administering social media background checks. Information not related to the job should not be forwarded to the hiring manager.

For human resource managers it is appealing to have a wealth of information on candidates. Viewing social media profiles can be a quick way to identify poor communication and grammar skills, offensive photos and remarks, and an exaggerated resume. However, a city must keep in mind that viewing an applicant's social media profiles may put them at risk for violating: GINA, Title VII of the Civil Rights Act, American's with Disabilities Act, the Pregnancy Discrimination Act, and the Age Discrimination in Employment Act. In addition, a city can open itself up to disparate impact and disparate treatment claims.

Social Media: Disparate Impact

Reference Number: MTAS-1613

General Employment Discrimination

In 1971 the Supreme Court formally recognized two primary types of employment discrimination, disparate treatment and disparate impact. Cities using information obtained on social media sites to make hiring decisions may be vulnerable to disparate impact and disparate treatment claims.

Disparate impact involves an employer with a practice that has an unintended, but unfair impact on a protected class. An example of disparate impact would be an employer who relies heavily or solely on social media for recruitment which will exclude certain segments of the applicant pool (i.e., older applicants) that may not use social media in the same manner as another group of applicants.

Employers who solely use social networking as a means to hire or recruit applicants may be vulnerable to a disparate impact claim. Disparate impact can occur when a city uses social media as a sole means to evaluate candidates or a when a city only considers applicants who use social media. It can also become an issue when a city shows preference for those applicants who have a more favorable online status as opposed to those who have a limited presence on social media. Perhaps the most concrete risk of disparate impact is that the population on social media networks is not representative of the real applicant pool that exists. This means this practice may be unintentionally excluding certain classes of applicants such as males, minorities, or older Americans. When using social media as a tool for recruiting and hiring, municipalities must be mindful of the fact that there is a marked difference in social media use in varied demographic groups, and even within those demographic groups there is a difference in the types of users that access different social media sites.

Social Media: Disparate Treatment

Reference Number: MTAS-1614

Disparate treatment involves intentionally different, and often adverse, treatment of individuals based upon their membership in a protected class. An example of disparate treatment may be the evaluation of applicants in a particular protected class through social media and others through another process. This may happen when a city lacks a recruitment plan and neglects other forms of job advertising. Employers should not use the information found on social media sites in an inconsistent way, or in a different way, for applicants applying for the same job. In other words, if you are going to use social

media to make judgments about one candidate class, you should look at the same information for all applicants and document this process.

Social Media: Federal Employment Laws

Reference Number: MTAS-1615

As employers, applicants, and employees increasingly use social media for employment purposes it should be noted that cities must consider all applicable local, state, and federal laws in using these media forms. Remember, employment laws are currently the same for an employer who uses social media for any hiring procedure as an employer who does not use social media in the hiring process.

Here are applicable employment laws:

- USERRA / State Military Laws
- TITLE VII
- ADA
- ADEA
- PDA
- GINA

Federal Employment Laws

- ***Title VII of the Civil Rights Act*** prohibits discrimination based on race, color, sex, national origin, or religion. This federal law applies to local government with at least 15 employees. Additional protections have been extended to include pregnancy discrimination and sexual harassment.
- ***Americans with Disabilities Act of 1990 (ADA)*** prohibits employment discrimination based on disability. Also requires employers to make reasonable accommodations to persons with disabilities.
- ***Age Discrimination in Employment Act of 1967 (ADEA)*** prohibits employment discrimination based on age forty and up. This applies to applicants as well as employees.
- ***Pregnancy Discrimination Act of 1978*** prohibits discrimination on the basis of pregnancy, childbirth, or related medical conditions.
- ***Genetic Information Nondiscrimination Act (GINA)*** This legislation prohibits employers from using individuals' genetic information when making hiring, firing, job placement, or promotion decisions. It also prohibits improper use of genetic information for purposes of health insurance and employment decisions. GINA broadly defined genetic information to include family members of employees which initially left employers concerned about the implications of using social media to interact with employees.

Social Media: Invasion of Privacy

Reference Number: MTAS-1617

You should be familiar with local, state, and federal rules concerning invasion of privacy. Under no circumstances should a city ask for log on identification or passwords, or use someone else's passwords to access employees' or applicants' social networking accounts. A popular restaurant chain found itself in court after asking employees for this information on a private "group" designed for the purpose of venting about work. The employees won the case because the employer gained unauthorized access to the social network by forcing employees to provide their user credentials.

In another situation, a city in Montana found itself on the front page after asking applicants to provide their user names and passwords as part of the hiring process and background check. The news of this went viral, and city officials promptly retracted their stance. Surprisingly, this was not an isolated incident that only occurred in this municipality.

The courts have stated that employers should not attempt to gain unauthorized access to private social networking profiles/groups for the purpose of spying on employees. Employers should be reminded that there is a risk in attempting to access employee/applicant content that is unauthorized or intended to be private.

Social Media: Off-Duty Behavior

Reference Number: MTAS-1618

A legal grey area exists when it comes to a public employer's ability to regulate an employee's use of social media when he/she is off-duty. In some instances, an employee's social media presence off-duty may be problematic and even dangerous for a municipality. An example of this is when police officers post inappropriate photos of themselves online while identifying themselves as public safety officers or undercover officers or post information that could compromise the integrity of a law enforcement investigation. These issues have prompted many police and fire departments to adopt a department-specific social networking policy.

A municipality may want to consider the following in creating their social media policy:

- Authorized use of uniforms, insignia, emblems, municipal logos and anything related to municipal business
- Anonymous "blogging" or information sharing regarding municipal business
- Discussing work issues or personal thoughts about municipal strategies online
- Protection of sensitive information
- Security of undercover public safety work (present and future) such as an employee's future capacity to move into an undercover position

A municipality should have clear policies in place to address certain off-duty online activity of employees. In public service, the off-duty behavior standard may be set high, particularly for public safety employees.

Because the test for determining whether an employee's off-duty use of social media can result in discipline, or is truly speech that is protected under the first amendment, is fact specific, it is important for you to consult legal counsel and your human resources professional before disciplining an employee for this type of conduct.

Social Media: Disciplining Employee for Online Activity

Reference Number: MTAS-1619

While each case is different and you should rely on the advice of your legal counsel, here are some questions that you should ask before disciplining or terminating an employee for their social media activity.

- Do we have a policy on social media?
- Did this employee's conduct relate to his/her job?
- Is the speech in question protected by law?
- What do we have that constitutes as "proof" of employee misconduct?
- Did the employee admit to the behavior?
- What valid policies, or local, state, or federal laws did the employee violate?
- How have we treated other employees in similar situations?
- Did you consider the issue of location-based services and time stamping (creation/modification time)?

MTAS has received a fair number of questions concerning Workers' Compensation claims and employees use of social media while on approved Workers' Compensation leave. A common issue that arises is the conflict between an employee's activities shown via social media and the employee being

out on leave due to what has been reported as an illness or workplace injury. Before your municipality approaches an issue related to social media and workers' compensation consider the following.

Workers' Compensation

- Did the municipality obtain the information about the employee ethically and legally and within the social media site's term of use and within city policy?
- How will this action affect the current workers' compensation claim?
- If the employee is on workers' compensation, did the claims administrator deny claims based on this information?
- If the employee is on workers' compensation, is the employee being formally charged with fraud?
- Is the municipality using the time stamp or the date and time posted as their primary concern or is the content itself a violation of policy?

While some conduct may be viewed as frowned upon, there may be no legal basis for discipline. Before disciplining an employee for off-duty behavior on social media, or behavior observed on social media that conflicts with claims filed by or leave taken by the employee, review your personnel policies as well as your social media policy.

Location-Based Reporting and Time Stamps

The municipality should be mindful that the time stamp (creation/modification time) that appears on social media sites is not an accurate account of what the person was doing at that time. Most social media sites now let users control and often pre-set the time and date that a post is made and user settings can dictate incorrect times based on time zones. In addition, social media sites that use a GPS tracking or location based reporting are commonly incorrect.

Harassment

Social networking provides yet another vehicle for workplace harassment and bullying. Workplace harassment can take place via the internet just as it can in person or in writing. If a municipality is using social networking to promote its own interests, the social media venues should be closely monitored for harassment and potential acts of violence.

Upon discovering an employee is using social media to harass another employee, the municipal employer has a legal duty to address the situation within a reasonable period of time. Employers should treat these incidents just as seriously as an in person harassment situation.

Recordkeeping

If a municipality is accessing social media profiles as a means to make hiring decisions, the information retained is subject to the municipality's record-keeping policies and practices and may be subject to the Tennessee Public Records Act. If a municipality prints a profile, it is likely to contain information that should not be considered in the hiring process. The EEOC's current guidance is for employers to continue to structure non-discriminatory recruitment and selection processes and consistently focus on the job qualifications of all applicants, regardless of the information available to the employer about the applicant through social media. However, if you are using social media profiles as a means of screening applicants, that information should be maintained as a part of your record keeping until such time as it can be destroyed pursuant to the municipality's records retention schedule.

DISCLAIMER: The letters and publications written by the MTAS consultants were written based upon the law at the time and/or a specific sets of facts. The laws referenced in the letters and publications may have changed and/or the technical advice provided may not be applicable to your city or circumstances. Always consult with your city attorney or an MTAS consultant before taking any action based on information contained in this website.

Source URL (retrieved on 01/23/2020 - 7:00am): <https://www.mtas.tennessee.edu/reference/social-media-legal-issues>



Municipal Technical Advisory Service
INSTITUTE *for* PUBLIC SERVICE