

# SOCIAL MEDIA & GOVERNMENTS – LEGAL & ETHICAL ISSUES

JULIE A. TAPPENDORF, ANCEL GLINK

## I. INTRODUCTION

## II. BENEFITS OF SOCIAL MEDIA

- A. Timely and Cost Effective Communication
- B. Creating Real-Time Public Record of Project Information
- C. Increased Public Participation & Encouraging Social Activism
- D. Garner Support for Municipal Projects
- E. Publicize Meetings and Hearings
- F. Public Safety Information
- G. Networking and Marketing

## III. LEGAL ISSUES

- A. Open Meetings Act
- B. Freedom of Information Act and Records Retention Laws
- C. First Amendment
- D. Discrimination
- E. Copyright Issues
- F. Privacy

## IV. EMPLOYEE USE OF SOCIAL MEDIA

- A. Constitutional Protections
- B. Hiring Decisions
- C. Discipline of Current Employees
- D. Employer Requests for Social Media Passwords

## V. ETHICS AND USE OF SOCIAL MEDIA BY ATTORNEYS

- A. Solicitation and Advertising
- B. Practice and Specialization
- C. Jurisdiction
- D. Attorney-Client Relationship
- E. *Ex Parte* Communications
- F. Contact with Witnesses and Represented Parties

## VI. IMPORTANCE OF A SOCIAL MEDIA POLICY

### APPENDIX A - Checklist for Drafting a Social Media Policy

## **I. INTRODUCTION**

Social networking describes a set of Internet tools that enable shared community experiences, both online and in person. These sites go beyond the more “passive” websites operated by governments and organizations. Each of the various social networking sites is tailored to a specific need and is designed to encourage active participation by both the member and his or her audience. For example, “Linked In” is marketed to businesses and professionals as a way to interact and form networks or “connections” with others. Facebook enables users to create a profile, update a status, include pictures, add “friends,” and post comments on the “walls” of personal or friend pages. Twitter allows people to connect with (or “follow”) a large number of users and post short notes of no more than 140 characters, called “tweets.” Instagram and Flickr allow users to post photos and Vine and YouTube allow videos, to share with others.

The growth of social media applications in the government context has an impact not only on government officials who use social media, but also the increasingly information-hungry general public, who expect local, state, and even the federal government to use these technologies to more effectively disseminate information and allow a forum for comment. In fact, social media provide the public sector a wealth of opportunity to communicate with the public, with interested stakeholders, and with each other about new proposals and ideas. Additionally, social media may be used by all parties interested in public sector decision making, including developers, applicants, individual advocates, non-profit organizations, and governmental entities.

However, the general benefits of the use of these fairly new technologies—which include the promise of greater transparency and greater public participation—must be weighed against the potential drawbacks, such as truthfulness and accuracy of posted information, the source of the posted information, and the longevity of inaccurate information in cyberspace. Additionally, there are a number of issues to consider when public officials and employees choose to utilize social networking tools, as well as a host of legal issues when organizations choose to create and host these sites.

## **II. BENEFITS OF SOCIAL MEDIA**

Social networking forums such as Facebook, MySpace, and Twitter all share information with a large number of Internet users. 72% of online adults have a profile page on a social networking site, a number that is in stark contrast to a 2005 study where only 5% of adults used social networking sites. However, this reliance on social media is also growing in older populations as well. The 45-54 age group is the fastest growing group on Facebook and Google+, and the fastest growing population on Twitter is the 55-64 year age bracket, up 79% in the last year.

Moreover, many citizens rely on the Internet and social media for much of their information gathering and communications, replacing more traditional media sources such as newspapers and television news reports with online options. Almost half of online adults say that they use social media to get information about their local community, and this number will surely grow in the future, as more younger users tend to rely much more heavily on the Internet—including social media—to get information.

With this rapidly growing user base, the public sector must be aware and willing to implement social media in at least some aspect of future plans and development. Social media offers governments a diverse array of benefits, as follows:

## **A. Timely and Cost Effective Communication**

Social media is a time and cost-effective communication tool for both governmental agencies and their constituents. Social media allows the public a direct link to government. People who receive their information online may not have to spend their time calling and stopping into government offices for information, completing Freedom of Information requests, or attending community meetings and workshops. In turn, government agencies spend less time dealing with requests from the public, and can communicate on any common concerns of their constituents in a more efficient manner.

The public can obtain information at virtually no cost as long as they have access to both a computer and the Internet. Similarly, governments realize savings, because they can use social media platforms to collect and distribute information about upcoming projects in a more cost effective manner than the traditional methods of postage and paper for newsletters, newspaper notices, community mailings, as well as finding space for community meetings and workshops.

## **B. Creating Real-Time Public Record of Project Information**

Social media offers a forum to post and obtain information quickly, but it also allows governments to create a record of that feedback in one place. Many social media platforms allow government agencies to post meeting minutes, records, project proposals, maps, applicable local laws and various other documents for public dissemination. Governments may also include links on their social media pages to direct constituents to their own website where more detailed records and information can be found. Governments can upload information from just about any location, and the public can, in turn, access this information from any location.

## **C. Increased Public Participation & Encouraging Social Activism**

The use of social media by governments has been called “the new public square” because of its impact on citizen participation in government activities. Using social networking sites can allow governments not only to keep up with the changing technology and be where their constituents are, but also to create an easy way for the public to participate. Social media provides information and a means of participation for those who may not otherwise be able to attend a meeting or hearing, to ensure that their opinion is heard.

## **D. Garner Support for Municipal Projects**

Arguably the most important step in any policy proposals by governments is to garner more support than the opposition. Many progressive ideas and policies by governments can be shelved remarkably early in the process when facing opposition—especially a well-organized opposition. This, combined with the multitude of social media platforms, makes it essential that local governments effectively campaign for new projects and proposals using social media to effectively disseminate information to the public. Governments can do this by methodically implementing a public relations campaign that relies heavily on social media.

## **E. Publicize Meetings and Hearings**

Social media can be used as a supplement to other more traditional methods of notifying residents and other interested parties of upcoming meetings, events and activities.

## **F. Public Safety Information**

Governments are beginning to use social media to inform citizens of emergency or public safety information.

## **G. Networking and Marketing**

Governments can use social media not only to discuss issues of concern and provide emergency information but also to market their governments to potential tourists. Social networking can also be used to redefine a larger city's image or spotlight a government. Social media can also be used to promote job seekers and match them with potential employers. Thus, social networking can not only impact government operations, but can also provide a tool for promoting the government that might attract tourism and business to boost the economy.

## **III. LEGAL ISSUES**

Despite the growth and overall positive reports of how the public sector has embraced social media, there are a growing number of legal issues that governments will face in their use of social media.

### **A. Open Meetings Act**

The policy behind open meetings laws is that government decision-making and legislation should be made openly, and not in secret or closed-door session, so that the general public can be fully informed and provide input regarding the proposed actions of the decision-making body. To this end, open meetings laws require that all meetings of decision-making bodies provide notice and be open to the public (with certain statutorily provided exceptions).

Communications which take place on a social media platform have the potential to run afoul of open meeting laws. Without realizing it, these communications: "friending," "tweeting," "messaging," "blogging" - all considered informal by most people's standards - can constitute a "meeting" under most open meeting law regimes.

Because of the "newness" of social networking by government officials, there is little guidance from the courts. The Florida Attorney General, however, has issued an opinion that a government social media site would likely implicate the state open meetings requirements, among other sunshine laws. Given the potential for criminal penalties in some states' open meetings laws government officials should be advised to avoid contemporaneous discussions or debates of public business (such as the benefits or impacts of a particular development proposal) on social networking sites or in chat rooms, and should ensure that their social networking interactions comply with applicable open meetings laws.

### **B. Freedom of Information Act and Records Retention Laws**

Communication via a government-sponsored or maintained website or social media site (including comments and other postings) is likely to be subject to public records laws if it concerns government business. While the Freedom of Information laws may not specifically mention social media records, some states that have encountered this issue have determined that these records are subject to FOIA. For example, the Florida Attorney General has opined that information on a government social networking site would be subject to public disclosure and records retention laws

if the information was made or received in connection with the transaction of official business by or on behalf of the public agency. Thus, governments must be aware that state law may require that these records be retained indefinitely or that permission must be sought prior to destroying them under public records law, and that the records must often be provided upon request. A good rule of thumb is that governments should avoid creating new material on social networking sites and instead use existing material that is already maintained for local records law compliance.

### **C. First Amendment**

One of the most useful features of social media is the ability for interaction between the public and the government. However, this interactive aspect can quickly become a potential minefield of legal issues for governments, particularly where comments and speech are involved. As this area of law is yet undeveloped, the public sector should proceed with caution so as to avoid running afoul of the First Amendment.

Whether a social media site is considered a “public forum” is an open question, raising concerns as to whether a government can remove allegedly objectionable Facebook comments without implicating First Amendment protections. The classic forum analysis will provide different protections to speech and other First Amendment rights depending on the forum in which such speech or rights arise.

A traditional public forum includes places that are traditionally used for assembly, debate, and other “expressive activities,” including streets, sidewalks, and parks. Traditional public forums are places that have “the physical characteristics of a public thoroughfare, . . . the objective use and purpose of open public access or some other objective use and purpose inherently compatible with expressive conduct, [and] historical[ly] and traditional[ly] ha[ve] been used for expressive conduct.” A government creates a public forum “only by intentionally opening a non-traditional forum for public discourse” and “does not create a public forum by inaction or by permitting limited discourse.” If a government tries to place restrictions on the content of speech in a traditional public forum, these restrictions must be necessary to serve a compelling government interest.

A designated public forum is a nonpublic forum that is not historically open to speech and assembly-related activities but that the government agency has purposefully opened up for public dialogue on a limited or permanent basis. Examples of a designated public forum include university meeting facilities, municipal theaters, and school board meetings. Although the government is not required to maintain designated public forums on a permanent basis, the government is bound by the same standards of traditional public forums as long as it does keep them open. Government may restrict content-neutral speech as long as it is a narrowly tailored restriction that leaves open alternative channels of communication, and any content-based speech restrictions must withstand a strict scrutiny analysis, i.e., the restrictions are necessary to achieve a compelling government interest. Analogizing this to social media sites, some argue that a government Facebook site is a designated public forum once the government has opened up its site to public comments.

There is a subset of designated public forums known as “limited public forums.” A limited public forum generally includes the same setting as designated public forums, but the government limits and restricts the discourse to certain speakers and certain subjects. The main difference between these two standards is the protection afforded to the speech—in limited public forums, speech restrictions need only be reasonable and viewpoint neutral. In a limited public forum, a government

agency can freely restrict and reserve access to the forum to certain topics and certain groups as long as the restriction is not because of the opinion or ideology of the speaker or group. A government must be careful to monitor and enforce the restrictions and limits on the topics and groups as designated or run the risk of having the forum deemed a designated public forum subject to the stricter test. Courts have found city council meetings to be limited public forums. Government has the power to remove people from meetings as long as they are *actually* disruptive. For example, a public agency was found to have acted properly to eject a member of the public when he continued to actively disrupt the meeting by yelling, interrupting, and trying to speak over the members of the board when it was not time for public comments. On the other hand, a government erroneously ejected a man from a city council meeting when he disagreed with the council members by silently giving them the Nazi salute.

At the other end of the spectrum lies the government speech doctrine, which protects the government against First Amendment claims in situations where the government has complete control over the message that it disseminates and retains the right and ability to exclude others. This doctrine was applied by the Fourth Circuit Court of Appeals to a school district website. In *Page v. Lexington County School District One*, 531 F.3d 275 (4th Cir. 2008), a county resident brought an action against a school district seeking access to, among other things, the school’s website to disseminate information that supported upcoming state legislation. The citizen took issue with the school district’s use of its own website to advocate against upcoming legislation—often through linkage to third-party publications. The resident claimed that by including links to other websites, which could be updated without the school district’s consent or approval, the district had incidentally created a “limited public forum.” The court rejected the challenger’s argument, finding that because the school “wholly controlled its own website, retaining the right and ability to exclude any link at any time” as well as including a disclaimer on the website addressing this exact situation, there was no limited public forum created; and further, the school was protected for its views under the government speech doctrine.

Some commentators suggest that government social media sites should be treated the same as websites. The U.S. Court of Appeals for the Fourth Circuit appears to anticipate that issue in the *Page* decision, as follows:

Had a linked website somehow transformed the School District’s website into a type of “chat room” or “bulletin board” in which private viewers could express opinions or post information, the issue would, of course, be different. But nothing on the School District’s website as it existed invited or allowed private persons to public information or their positions there so as to create a limited public forum.

The *Page* decision should give pause to governmental agencies as it suggests just how easily a nonpublic forum can be transformed into a limited public forum—merely by providing a link to some page that allows private users to express opinions or post information.

A recent case may eventually shed some light on this open issue of whether social media is a public forum (traditional, designated, or limited) or is government speech. In *Hawaii Defense Foundation v. City of Honolulu, et al*, a legal defense group sued the City claiming it violated its First Amendment rights by removing comments posted on the city police department’s (HPD) official Facebook page and banning those individuals from the site. The lawsuit claims that the HPD’s Facebook page was a traditional public forum, like a public park. At the very least, according to the

plaintiffs, the City had created a designated public forum when it set up its Facebook page and allowed comments to be posted. According to the complaint, the HPD had removed comments that were critical of the police department solely based on the content or viewpoint of the speech rather than for violation of the HPD's Facebook use policy. That policy prohibits comments that are obscene, sexually explicit, racially derogatory, or defamatory, solicit or constitute an advertisement, or suggest or encourage illegal activities. The plaintiffs seek a declaratory judgment that the City's administration of its Facebook page, specifically its removal of plaintiffs' comments, violated the First Amendment. The lawsuit also claims that the City's ban of certain plaintiffs from posting comments violated their due process rights under the Fourteenth Amendment.

While we do not yet know what the City's defense will be (and may not know if the case ultimately settles), it is likely that the City will argue that its Facebook page involves government speech and should not be subject to a forum analysis. This case certainly bears watching to see what analysis the court will use and, whether the court will find that the City's Facebook page is a public forum or government speech.

#### **D. Discrimination**

Governments who use social media must be aware of, and address the fact that some people are unable to access the Internet for a variety of reasons. Although this can stem from many situations, governmental agencies need to make sure that they are not using social media, as well as the Internet, in a manner that actually hampers the access of information from certain subset groups of people.

A variety of statutes affect governmental agencies which use social media, including the Americans with Disabilities Act and the Rehabilitation Act. Government bodies are obligated by law to provide disabled individuals with "equal access" to information posted on social networking sites, unless it would "pose an undue burden" or that doing so would "fundamentally alter the nature of the provider's programs." Thus, governments who use social networking sites should have an alternative way to provide the information to disabled individuals, such as sending it through the mail or reporting it by phone.

Furthermore, governmental agencies must also take care not to overuse social media, and perhaps incidentally alienate segments of the populations which do not traditionally use social media. Data shows that there is a discrepancy in the use of the Internet by income, race, age, and education level, raising concerns that the use of social networks to share information and solicit input on government issues and projects might reach a less diverse group of people. If government officials are using social networking sites as the only means to get information and receive input, a significant number of citizens may be underrepresented.

#### **E. Copyright Issues**

Governmental entities also need to be careful about what they post on social media pages to avoid potential copyright liability, as well as protect their own original work-product. Photos and video should be produced by the organization or individual who posts the media. If copyrighted materials are used, the poster should make sure it obtains and maintains physical records of the copyright licenses. All users of social media sites should also be aware that some social networking sites (such as Facebook) have terms of use in place that state that by posting intellectual property on Facebook,

an individual grants Facebook a “non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content” that is posted. Consequently, users should be cautious and sensitive to the content uploaded on these sites.

## **F. Privacy**

Many social media platforms allow users to set their own privacy settings, which often cover a number of areas including who view their profile, who can post comments and other content on the profile, and who can search for their social media page or channel. Although the vast majority of these privacy concerns apply to individual users, public sector users should be equally as conscious. Everyone who uses social media should begin with the assumption that everything posted on a government site is likely a public record. Privacy issues involving social media are being slowly developed through case-law, and are still considered an open question subject to further explanation.

Also, be aware that if a governmental entity requires people to register to use a government social networking site, it must carefully consider what information the registrant must provide (name, address, phone number, email, screen name), who will maintain the information, and whether others participating in the discussion will have access to this information.

## **IV. EMPLOYEE USE OF SOCIAL MEDIA**

Public employers continue to walk a tightrope when regulating the use and content of the electronic communications of its employees and when taking employment action based on the use or content of its employees’ electronic communications. The law is well settled that a public employee has a limited or no expectation of privacy in their office, desk, locker or even their telephone calls at work. Unfortunately, the law moves slowly and is far from addressing the balance of rights of employees and employers in the context of electronic communications.

### **A. Constitutional Protections**

Public employees do not surrender all of their First Amendment rights, particularly their speech rights, merely because they are employed by the government. However, the speech of public employees can be subject to certain restrictions by the government, because it has a different—and more significant—interest in regulating the speech of its employees than the general public.

The U.S. Supreme Court has outlined a two step analysis for determining whether the speech of public employees is protected by the First Amendment. First, it must be determined whether the employee spoke as a citizen on a “matter of public concern.” If the speech is a matter of public concern, then the court must engage in the *Pickering* balancing and decide whether the government was justified for treating the employee’s speech differently from the general public.

Courts decide whether speech is a matter of public concern based on “the content, form, and context of a given statement, as revealed by the whole record.” Of these three factors, the content of the statements have generally been acknowledged to be the most important, although the form and context can help make a statement one of public concern if the speech at issue occurs in an unconfined space. Matters which have been found to be of the public concern include: speech relating to public safety and policy protection; governmental wrongdoing and misconduct; or speech which seeks to expose wrongdoing by government officials.

*Pickering* balancing has been used in Internet postings. In *Curran v. Cousins*, 509 F.3d 36, 49 (1st Cir. 2007), a corrections officer was terminated for postings he made on a union website. This website was owned and controlled completely separately from the public employer, and featured a public discussion board which allowed registered users to “post comments and statements. Any person with access to the Internet—whether a member of the union or not—could register, post, and read messages.” The officer, who had been suspended a week earlier for “threatening and menacing” co-workers, posted messages to the website that made unfavorably comparisons to the current sheriff, and his personnel decision-making to Adolf Hitler and the Nazis during World War II. The employee was thereafter fired due, in part, to his posting on the website. The First Circuit did note that although most of the content of the posting was not a matter of public concern, a part of the posting which addressed the sheriff making personnel decisions based on political affiliations rather than merit was a matter of public concern. However, in balancing the speech of the employee and the later actions of his employer to fire him, the court found that the government was plainly justified in firing the employee. In the posting, the employee referenced the plot of Hitler’s generals to kill him, and urged a similar plot by analogizing the current sheriff to Hitler. Further, the court found that “[s]peech done in a vulgar, insulting, and defiant manner is entitled to less weight in the *Pickering* balance.”

One case deciding the issue of whether employee activities on social media are protected speech under the First Amendment involved employee political activities. That case involved employees of the local sheriff who supported the sheriff’s opponent in the election. To the employees’ misfortune, their supported candidate lost the election, and the sheriff terminated them. The employees sued, claiming that the sheriff retaliated against them in violation of their First Amendment rights by terminating them for engaging in protected speech activities - in this case, clicking “like” on the candidate’s Facebook page. The district court judge ruled in favor of the sheriff, finding that the mere action of clicking “like” on Facebook was not “speech.”

The employees appealed to the U.S. Circuit Court of Appeals, Fourth Circuit. That court issued its opinion in September of 2013 reversing the district court and finding that the employees did engage in protected speech activities in their conduct on the sheriff’s opponent’s Facebook page. *Bland v. Roberts* (U.S. Court of Appeals, 4th Cir. September 18, 2013).

First, the court reviewed the Supreme Court political speech retaliation cases in determining which of the employees were protected and which employees were exempt as occupying a “policymaking or confidential position.” Under the Supreme Court’s decisions in *Elrod v. Burns* and *Branti v. Finkel*, a public employee who has a confidential, policymaking, or public contact role has substantially less First Amendment protection than a lower level employee. The purpose of the Elrod-Branti test is to ensure loyalty with employees in certain policymaking or confidential positions. In this case, the court determined that the plaintiff deputy sheriffs were not in policymaking positions where their political allegiance to the sheriff was a job performance requirement.

Second, the court looked at the conduct of the employees to determine whether their activities (supporting the sheriff’s opponent on the opponent’s Facebook page) were a substantial motivation for the sheriff’s decision not to reappoint the employees. The court looked at the sheriff’s conduct as well, including his statements to employees that those who openly support his opponent would lose their jobs, and specifically referencing his disapproval of the decision of some employees to support his opponent’s candidacy on Facebook.

Third, the court addressed the question whether the employees' activities were speech. As noted above, the district court had ruled that merely clicking "like" on Facebook was not speech. The appellate court disagreed, however, stating that "clicking on the 'like' button literally causes to be published the statement that the User 'likes' something, which is itself a substantive statement." Particularly in this context, clicking "like" on a candidate's Facebook page sends a message that the user approves the candidacy. The court found this to be pure political speech, as well as symbolic expression - a "thumbs up" symbol that the user supports the campaign by associating the user with it. As the court noted, liking a candidate's campaign page "is the Internet equivalent of displaying a political sign in one's front yard."

The lesson from the *Bland* case is that employers must be cautious in taking disciplinary action against an employee for the employee's social media activities that might be protected First Amendment speech. In this particular case, the comments and "likes" on Facebook were considered protected political speech.

## **B. Hiring Decisions**

Never has so much information about so many been available with the click of a mouse. Every prospective employer is interested to know everything that they can about a job applicant. And every employer knows that they might find something on the Internet which the applicant is reluctant to divulge in an interview. It may not be a matter of finding out "dirt" on the candidate, but just learning more about their likes, dislikes, lifestyle, thoughts and beliefs which may provide greater insight into their potential suitability as an employee. Nevertheless, the question arises as to what information from the Internet an employer can use when making hiring decisions.

Reliance on Internet information has become so common that we often forget that not all information obtained in Internet searches is completely accurate. Anyone can post information on the Internet and no assurance exists that it is all truthful. We have all heard about altered photos and intentionally planted misinformation which causes problems for an individual, to say nothing of the problems of those with common names or the same name as someone with a negative reputation. If searching for information on job candidates on the Internet, always remember that the information may not be truthful, accurate or reliable.

While it is not illegal to review public information about job candidates, it is advisable that candidates know of this possibility ahead of time. If candidates are aware that searches of social network and other Internet sites is part of the candidate review process, a decision based in whole or part on this information will not be inconsistent with their expectations. Thus, they will be less likely to claim that an adverse decision was the product of discrimination or other illegal basis.

Prospective employers can make employment decisions on any basis that is not an illegal basis. Examples of illegal considerations are those such as race, gender, and religion. Off duty conduct can be a relevant job qualification depending on the position for which the employee applies. For example, it may be relevant to the qualifications of a police officer whether that individual posts pictures of him or herself in situations which depict illegal activity. Evidence of gang affiliation may also disqualify a candidate from employment with law enforcement. Whether information gathered from electronic sources, or any other, serves to disqualify a candidate from public employment depends largely on the position which is sought and the type of behavior which is disclosed. On the other hand, public employers must take great care to avoid decisions based on

social network information related to religious affiliation, ethnic or racial information gathered only from these searches and other information which, if used, as a basis to deny employment would violate the law.

Finally, given the potential for inaccurate information gathered from social networks or other Internet sites, it is advisable to allow a candidate to provide explanation to any information gathered from these sources to ensure that a decision is not based on false information.

### **C. Discipline of Current Employees**

Evidence of misconduct related to work performance that is gathered from social network sites may be an appropriate basis for action against current employees. Like pre-employment considerations, the misconduct must impact, or have a nexus, to the reputation of the employer or the employer's ability to deliver services to the citizens. So, for example, the police officer or teacher who posts obscene pictures of himself or herself on their Facebook page, or photos of obvious illegal conduct, likely serves an appropriate basis for disciplinary action.

Government employers, like other bosses, are struggling with critical social media posts by employees. Can an employer terminate or discipline a worker for complaining about his or her boss or company on Facebook? Will social media policies protect an employer? The answers to these questions are not yet clear, because there is little case law on this issue. However, the National Labor Relations Board (NLRB) has been active in this area recently. While the National Labor Relations Act does not apply to government employers, the NLRB rulings can provide government employers with some guidance.

In one case, the NLRB ruled that a nonprofit employer unlawfully discharged five employees who had posted comments on Facebook relating to allegations of poor job performance that had been previously expressed by one of their coworkers. The workers were found to be engaged in "protected concerted activity" because they were discussing terms and conditions of employment with fellow co-workers on Facebook. The NLRB cited the *Meyers* ruling that an activity is concerted when an employee acts "with or on the authority of other employees, and not solely by and on behalf of the employee himself." In this case, the discussion was initiated by one worker in an appeal to her coworkers on the issue of job performance, resulting in a "conversation" on Facebook among coworkers about job performance. The NLRB ruled similarly in a number of other cases.

In another case, however, the NLRB ruled that a reporter's Twitter postings did not involve protected concerted activity. Encouraged by his employer, a reporter opened a Twitter account and began posting news stories. A week after the employee posted a tweet critical of the newspaper's copy editors, the newspaper informed the employee he was prohibited from airing his grievances or commenting about the newspaper on social media. The reporter continued to tweet, including posts about homicides in the City and a post that criticized an area television station. The newspaper terminated the reporter based on his refusal to refrain from critical comments that could damage the goodwill of the newspaper. The NLRB found that the employee's conduct was not protected and concerted because it (1) did not relate to the conditions of employment and (2) did not seek to involve other employees on issues related to employment. The NLRB issued a similar ruling in a case involving a bartender who posted a Facebook message critical of the employer's tipping policy, finding the posts mere "gripes" that are not protected.

Two recurring themes have come out of the NLRB rulings. First, individual gripes or venting by employees is not protected and employers can discipline, and even terminate, employees for this conduct. Second, the NLRB is taking a very narrow view of social media policies and striking down a number of policies for being overbroad where the policies could be interpreted to prohibit protected conduct.

What does this mean for government employers? First, employers must be cautious in disciplining or terminating employees for critical posts on social media sites. An employer should ask itself whether the posts are "protected and concerted activity" or merely constitute "gripes" about an employer that are not protected? Second, an employer should review its social media policy to make sure it is not overbroad in prohibiting protected activities. Finally, an employer should be careful not to enforce social media policies in an arbitrary or discriminatory manner.

#### **D. Employer Requests for Social Media Passwords.**

It has become common practice for public and private employers to review the publicly available Facebook, Twitter and other social networking sites of job applicants as part of the vetting of candidates in the hiring process. However, because many social media users have privacy settings that block the general public (or non-friends or followers) from viewing their complete profile, some employers are asking candidates to either turn over their passwords or log on to their social media accounts during the interview.

Because an applicant can decide not to apply for a particular job, some employers have argued that it is neither an invasion of privacy nor a violation of constitutional rights to ask for this information during the hiring process and if applicants refuse to provide the requested information, employers are free to drop their consideration for hire. Nevertheless, the ACLU and others argue that this practice violates a candidate's right to privacy.

Until recently, there was no federal or state law expressly prohibiting this practice, although a few states have proposed or enacted legislation. Maryland became the first state to pass a law on the practice in April. Under this law, employers are prohibited from requiring employees and job applicants to "disclose any user name, password, or other means for accessing a personal account or service" electronically. Employers are also prohibited from refusing to hire an applicant for not providing access to this information. Similarly, employers are not permitted to terminate or discipline an employee for refusing to provide this information.

In addition to protecting the privacy of current and prospective employees, the Maryland law also provides employers with some protections. For example, employees are prohibited from downloading "unauthorized employer proprietary information or financial data" to personal accounts or to websites, and the law allows employers to investigate these activities to ensure "compliance with applicable securities or financial law or regulatory requirements." Additionally, employers are permitted to require employees to provide passwords and login information for non-personal accounts that are part of the employer's own systems, such as company e-mail accounts. The Maryland law took effect October 1, 2012.

The second state to pass a similar law is Illinois. Illinois P.A. 97-0875 prohibits public employers from seeking job applicants' social media passwords. The legislation allows candidates to file lawsuits if they are asked for access to sites like Facebook. Employers can still ask for usernames to view public information and monitor employee usage of social media on employer devices. The

new law became effective January 1, 2013. More than a dozen states have since enacted or proposed legislation similar to the Illinois and Maryland laws.

Employers should be cautious in using social media to discipline current employees. Unless there is an actual need to review an existing employee's social media profile, it may be difficult to find a connection between social media usage and the employee's right to hold their job.

## **V. ETHICS AND USE OF SOCIAL MEDIA BY ATTORNEYS**

Approximately two-thirds of lawyers are members of at least one social networking site, up from 50% just a few short years ago. An American Bar Association study found that 59% of law firms have a social media presence. Lawyers and law firms benefit from social media sites for the same reasons other businesses benefit – the dissemination of information about the firm and its attorneys and marketing the firm and its attorneys to potential clients. Many of the same legal issues that apply to government entities, organizations, and private companies also apply to lawyers and law firms, including copyright concerns, employment usage, among others.

While social media use is relatively new for lawyers and law firms, there have already been a number of ethical issues that have arisen from attorney use of social networking. Since each jurisdiction has its own ethical rules in place for attorneys practicing in the state, it is important to consult applicable rules and opinions of the practicing jurisdiction. However, a general discussion of the types of ethical issues that have arisen in the field of social media use by attorneys may be helpful to provide some guidance on these issues.

### **A. Solicitation and Advertising**

A lawyer may advertise services through written, recorded, or electronic communication, including public media. However, a comment to ABA Model Rule 7.2 cautions against real-time electronic solicitation of prospective clients. Thus, emails are probably acceptable, but not instant messaging or participation in chat rooms. Other forms of online solicitation may also be a violation of the prohibition of in-person, telephonic, or real time electronic solicitation.

### **B. Practice and Specialization**

A lawyer may not mislead or misrepresent his or her practice nor may a lawyer state or imply that he or she is certified as a specialist in a particular field of law. Lawyers should avoid providing legal advice in areas of the law where they are not experienced and should be careful not to misrepresent their practice area expertise and experience. In addition, some jurisdictions prohibit attorneys from self-identifying as an "expert" or "specialist" in a particular field of law. This rule can be tricky to follow on certain social media sites, such as LinkedIn, that ask for "specializations" in their profile forms, and allow users to "endorse" other users' skills and expertise.

### **C. Jurisdiction**

Lawyers are only authorized to practice in jurisdictions where they are licensed. Social media sites, blogs, listservs, and similar sites can make this difficult for an attorney with exposure to people across the country looking to the attorney for guidance on state-specific legal issues. A lawyer should be careful not to provide legal advice on these state-specific legal issues unless he or she is licensed in that particular jurisdiction.

## **D. Attorney-Client Relationship**

Just as attorneys must be careful not to inadvertently create an attorney-client relationship at a cocktail party, over the telephone, on an airplane, by email, and through a law firm’s “question and answer” page on its website, attorneys must also be careful not to create an attorney-client relationship when using social networking sites. An attorney-client relationship might be formed when an individual “reasonably relies” on an attorney’s advice through a blog post, listserv, or social networking site.

## **E. Ex Parte Communications**

Lawyers should be aware that judges also participate in social networking and may have access to a lawyer’s communications that might implicate the prohibition on *ex parte* communications on pending matters. For example, listservs may have thousands of participants and a harmless “inquiry” about a pending matter could be read by the judge who is assigned to that pending matter.

## **F. Contact with Witnesses and Represented Parties**

Social media can provide lawyers with a bonanza of valuable personal information from other users, which, in turn, lawyers can use when preparing for litigation or settlement discussions. This can lead to many ethical complications which lawyers may not anticipate during their investigations. When using social media to investigate another party, lawyers must be careful not to engage in deceitful behavior, such as asking a paralegal or co-workers’ to use their account to gain access to information about that witness. The Philadelphia, San Diego County, and New York City Bars have all issued opinions to place restrictions on lawyers seeking to “friend” potential witnesses.

Even when a lawyer uses their true identity to “friend” or follow another party through social media even more ethical concerns can arise. Ethical rules place restrictions on the communications lawyers make with third parties who are represented by counsel. For example, a lawyer cannot communicate about the proceeding with a represented party unless they have the consent of that party’s lawyer or a court order. This is the case even if the person consents to the communication—i.e., even if they accept, respond, or engage any friend requests or messages sent.

## **VI. IMPORTANCE OF A SOCIAL MEDIA POLICY**

Governments participating in social networking sites must start with the realization that what is posted on social networking sites is public information. That means that government employees and officers should not post information that neither they nor the government would want everyone to know. By realizing the public nature of the information being published, confusion, lawsuits, and other problems can be more easily avoided.

All governments that use any form of online communication should develop, implement, and enforce a website and social networking policy. That policy should include a well-defined purpose and scope for using social media, identify a moderator in charge of the site, develop standards for appropriate public interaction and posting of comments, establish guidelines for record retention and compliance with sunshine laws, and include an employee access and use policy. The government should also post express disclaimers on its websites reserving the right to delete submissions that contain vulgar language, personal attacks of any kind, or offensive comments that target or disparage any ethnic, racial, or religious group. Finally, the government should train



employees regarding appropriate use of social networking and how use might impact the employer.

In crafting a social media policy, an employer should be careful not to implicate the First Amendment rights of its employees nor violate any applicable federal or state employment laws protecting employees. An example of this type of situation involved a settlement between the National Labor Relations Board and an ambulance service in Connecticut that fired an employee in 2009 for venting about her boss on Facebook. The ambulance company argued that the employee's Facebook criticism violated the company's social media policy barring workers from disparaging the company or their supervisors. The NLRB argued that the National Labor Relations Act protects an employee's discussion of conditions of his or her employment with others and that co-workers comments on the employee's Facebook page implicated those protections. As part of the settlement, the company stated it would change its policy so it did not restrict employees from discussing work and working conditions when they are not on the job.

As discussed above, the NLRB has struck down a number of social media policies for being too broad, so employers should take care in crafting a social media policy that avoids these issues.

A government might also consider providing examples of acceptable or unacceptable conduct in both employee and public usage of social media to illustrate the type of conduct that is regulated and why a particular regulation is in place. In addition, all employees should be required to sign a written acknowledgement that they have received, read, understand, and agree to comply with the social media policy.

A checklist for drafting a social media policy can be found on Appendix A.

## Appendix A

### Checklist for Drafting a Social Media Policy

A government considering establishing a Facebook, Twitter, or other social networking site should first adopt a social media policy to govern the administration and monitoring of site content, set ground rules for public input and comments, and adopt policies for employee usage of social media.

#### 1. Purpose

The policy should contain a statement that the use of social media by the government entity is for the purpose of obtaining or conveying information that is useful to, or will further the goals of, the government.

#### 2. Approval and Administration

The policy should provide for an administrator to oversee and supervise the social media networking sites of the government. The administrator should be trained regarding the terms of the policy and his other responsibilities to review content to ensure that it complies with the policy and furthers the government's goals.

#### 3. Comment Policy

The policy should identify the type of content that is not permitted on a social media site and that is subject to removal. This might include comments that are not relevant to the original topic; profane, obscene, or violent content; discriminatory content; threats; solicitation of business; content that violates a copyright or trademark; and any content in violation of federal, state, or local law. The policy should also contain a disclaimer that any comment posted by a member of the public is not the opinion of the government. Finally, the policy should include language that reserves the right of the administrator to remove content that violates the policy or any applicable law.

#### 4. Compliance with Laws

The policy should include language regarding compliance with applicable federal, state, and local laws, regulations, and policies. It should be made clear that content posted on a government site is subject to freedom of information and record retention laws. In addition, content posted on social media sites may be subject to e-discovery laws. Finally, information that is protected by copyright or trademark should not be posted or maintained on a social media site unless the owner of the intellectual property has granted permission.

#### 5. Employee Usage Policy

A social media policy should clearly establish guidelines and boundaries to enable employees to anticipate and understand company expectations and restrictions regarding social media usage. Although each employer should create a social media policy tailored to the particular employer's workplace, the following are some suggested employee usage provisions:

- a. The policy should clearly communicate to employees whether social media use in the workplace will be prohibited, monitored, or allowed within reasonable time limits. The



policy should be careful not to excessively restrict the content of employee social media postings to the extent that “protected concerted activity” among the company’s employees would be prohibited. For example, a social media policy should not ban “inappropriate discussions” about the company, management, working conditions, or coworkers that would be considered protected speech in another form or forum.

- b. The policy should also caution employees that they have no expectation of privacy while using the Internet on employer equipment. If employees will be monitored, the policy should inform employees of such monitoring.
- c. The policy might also require employees who identify themselves as employees of a particular government or company to post a disclaimer that any postings or blogs are solely the opinion of the employee and not the employer.
- d. Employees should be advised that they should not use the government or company logo, seal, trademark, or other symbol without written consent of the administrator.
- e. The policy should also address the protection of confidential and sensitive government information, as well as personal information relating to government officials and employees, customers, or residents.
- f. Prior to taking any adverse employment action against an employee on account of the content of the employee’s social media posting, consider whether the employee’s comments (1) were posted on a public site accessible to a large number of people; (2) disclosed confidential information about the employer, its employees, residents, or others; or (3) were directed at coworkers in a serious effort to discuss working conditions or were simply a venue for the employee to vent personal frustration. Any decision to take adverse employment action against an employee on account of social media use should be made in consultation with legal counsel.
- g. Finally, all employees should be required to sign a written acknowledgment that they have received, have read, understand, and agree to comply with the social media policy.

# Julie A. Tappendorf

Partner



**Clients turn to Julie for her advice on the crucial day-to-day issues faced by governments and her expertise in social media, ethics, land use, and zoning litigation.**

## Chicago Office

140 S. Dearborn Street, 6th Floor  
Chicago, IL 60603

## Direct Phone

312.604.9182

## Email

[jtappendorf@ancelglink.com](mailto:jtappendorf@ancelglink.com)

## Practice Areas

Local Government  
Land Use  
Elections  
Land Use Litigation

## Education

J.D., University of Hawaii,  
William S. Richardson School of Law  
B.A., Illinois State University

Julie focuses her practice on local government and land use matters, including counseling clients on ethics, social media, elections, personnel issues, and sunshine laws. She represents governments and landowners in a variety of land use matters, including negotiating and drafting annexation and development agreements, drafting zoning and other land use and development regulations, negotiating economic development projects, and representing clients in land use disputes in state and federal courts.

Julie currently serves as Village Attorney for Gilberts, Lindenhurst, and Wadsworth, and counsel to the Glencoe Police Pension Board and the Library Integrated Network Consortium.

Julie is co-chair of Ancel Glink's land use practice and co-editor of the group's newsletter, *In the Zone*. Julie is also the author of the local government blog, [Municipal Minute](#) and social media blog, [Strategically Social](#).

Julie has written and lectured extensively on local government issues, including the book [Social Media and Local Governments: Navigating the New Public Square](#) (ABA, 2013) and [Development by Agreement: A Toolkit for Land Developers and Local Governments](#) (ABA, 2012).

Prior to her law career, Julie served for eight years in the United States Army, Military Intelligence Branch, as a Korean cryptologic-linguist.

## Experience

Particular highlights of her recent practice include:

- Advising communities on day-to-day legal issues relating to ethics, meeting procedures, and local records laws, including preparation of administrative policies relating to FOIA, social media, personnel, and zoning hearings
- Successfully defended a municipality in an action by property owners challenging the annexation of certain property, affirmed by the Illinois appellate court
- Completed numerous comprehensive rewrites of zoning, subdivision, sign, and other development regulations
- Negotiated a settlement of a complex breach of contract case to enforce a development agreement involving a mixed-use downtown development
- Assisting communities in adopting vacant property regulations, priority liens, and other tools to address the housing crisis

## Presentations

Julie is a frequent speaker at local and national conferences on a variety of topics such as:

- Social Media & Governments – Legal & Ethical Issues (APA, ABA, IMLA, IML, 2011-2013)
- First Amendment & Cyberspeech (IICLE, 2013)
- Unconstitutional Conditions Post-*Koontz* (Touro Law School, 2013)
- I was at a meeting 'til 2 a.m. last night! What did you do? (ILCMA, 2013)
- Development Agreements and Exactions (APA, 2012)
- A DIY Guide to Drafting Ordinances & Resolutions (Minus the Hourly Rate) (Illinois Municipal League, 2012)
- Land Use and the First & Second Amendments (ALI Land Use Institute, 2012)
- Vacant Properties and Foreclosures: Minimizing the Impacts and Maximizing the Opportunities (ILCMA, 2011)

## Publications

Julie has published on a variety of government and land use topics, including the following:

- Social Media & Local Governments: Navigating the New Public Square (ABA Press, 2013)
- “Ethical Considerations in the Use of Social Media for the Land Use Practitioner and Government Lawyer” (The Practical Real Estate Lawyer, September 2013).
- “Attorneys and Social Media: An Ethical Minefield or Professional Boon?” (IMLA, Jan/Feb. 2013)
- Development by Agreement: A Tool Kit for Land Developers and Local Governments (ABA Press, 2012)
- Planning and Control of Land Development: Cases and Materials, Ninth Edition (LexisNexis, 2011)
- “To Tweet or Not to Tweet: Use of Social Networking in Land Use Planning and Regulation,” Zoning and Planning Law Report (May 2011)
- Bargaining for Development (ELI, 2003)