CITY OF MADISON
CITY ATTORNEY'S OFFICE
Room 401, CCB
266-4511

May 7, 2019

MEMORANDUM

TO: Members of the Common Council

FROM: Michael P. May
City Attorney

Roger A. Allen
Assistant City Attorney

SUBJECT: Use of Social Media by Government Officials

Summary of Legal Considerations

This memorandum addresses the significant legal considerations that arise when government officials use social media in their official capacities. This memorandum does not address the significant practical issues, such as storage, access, functionality, interfacing, data mining, etc., that must be considered when employing social media. It also does not address use of social media by government officials in their purely private capacity; it is often difficult to separate out what is a private use versus an official use.

Government officials must comply with significant state and federal laws when using social media. Use of social media by a government official is distinctly different from personal use of social media by a private individual. Government officials, unlike private individuals, must comply with the First Amendment to the U.S. Constitution, the Americans with Disabilities Act (ADA), the Wisconsin Open Meetings Laws (OML), and the Wisconsin Public Records Laws (PRL). Additionally, government officials should be cautious on clicking through the terms and conditions of service (TOS). Acceptance of such TOS can create a legally binding contract that is at odds with the state and local contracting laws.

A nascent and emerging area of concern is the development of data privacy laws both within the United States and internationally (such as the European Union General Data Privacy Regulation). While these laws are more likely to be of primary concern to the social media platform operators, the development of these laws should be closely monitored.

Applicable City Policies

City employees and City agencies are obligated to comply with APM 3-13, Web Linking Policy and APM 3-16, Social Media and Department Websites Policy. Alders are advised of the Common Council Social Media Policy (August 2011). Copies of these policies are attached to this memorandum.

First Amendment Considerations

Use of social media has become ubiquitous. Most government officials will use social media in both their personal and professional capacities. Care must be exercised to ensure that the personal use is just that: the sharing of personal information with only family members and close personal friends. Those officials entering public service should review their social media contacts to ensure that this maxim is observed.

When a government official opts to use a social media platform to communicate with the general public, that government official loses the ability to control who may access that message and, to a very large extent, what those persons may post to the social media platform. Recent case law establishes that the interactive portions of social media platforms constitute designated public forums where viewpoint discrimination is prohibited and presumed to be unconstitutional.[1] Thus, any person has a constitutional right to access such a website and to post their comments. A government official may not block any person, nor may they alter nor delete comments that they disagree with or find objectionable. While it is possible to develop content neutral rules for use of such an expressive forum[2], such rules should be reviewed and approved of by the Office of the City Attorney. This step should be taken prior to the use of the social media platform and prior to the implementation of such rules. Additionally, any person who is banned, blocked or otherwise denied access to the platform or whose comments are altered, amended or deleted, may have due process rights to appeal such actions.[3] They also might have a claim for violation of their civil rights.

Public officials should be cautious when selecting social media platforms. Some platforms may have eligibility requirements that equate to impermissible speaker or viewpoint discrimination.[4]

---

1 See *One Wisconsin Now v. Kremer*, 354 F.Supp.3d 940, (WD WI 2019), pp. 953-954; *Knight First Amendment Institute at Columbia University v. Trump*, 302 F. Supp.3d 541 (SD NY 2018), pp. 572-7; *Leuthy v. Maine*, 2018 WL 41344628 (D. Maine 8/20/2018).

2 While "viewpoint discrimination" is always prohibited, some restrictions are permissible if they are narrowly tailored to promote a content neutral and compelling state interest. *Rosenberger v. Rector & Visitors of the Univ. of Va.*, 515 U.S. 819, 830-31, 115 S.Ct. 2510. 132 L.Ed.2d 700 (1995).

3 Our review of existing case law was unable to locate any cases definitely describing the parameters of such a post-deprivation proceeding. This is an area that we will continue to monitor. However, current policies need to be amended to provide for due process post-deprivation appeals.

4 "For example, if the government chose as its electronic platform a social media site that allowed only registered members of one political party to post and comment, there would seem to be a compelling argument that he government's selection of that social media site violated the First Amendment rights of members of other political parties, even if the partisan restriction was imposed by the private company, not the governmental body." *Davison v. Randall*, 912 F.3d 666, 291 (4th Cir. 2019).

Or, they may employ tactics or procedures that equate to such impermissible restraint of free speech. For example, the City does not use NextDoor.com (NextDoor). NextDoor employs a system of geographically determined "electronically fenced neighborhoods". Only persons within the geographic boundaries of these neighborhoods may sign up for service and comment on the platform. The first neighborhood resident that contacts NextDoor gets to define the physical boundaries of that neighborhood on the NextDoor website. That person then becomes a "NextDoor Lead" and is tasked with policing the communications within their NextDoor "neighborhood". "NextDoor Leads" have the authority to remove communications/posts, terminate discussions and disable replies to posts, remove events from the neighborhood calendar, "mute" neighbors, adjust neighborhood boundaries, verify "unverified" members and select additional "NextDoor Leads." There are no qualifications or training required for becoming a "NextDoor Lead". There does not appear to be any direct oversight or limitations upon the censorship powers of "NextDoor Leads". It appears that "NextDoor Leads" can arbitrarily delete any post or silence any member without explanation or review. Thus, if a NextDoor Lead wishes to define a neighborhood so as to exclude a certain demographic, they appear able to do so. If a NextDoor Lead wishes to ban someone because of their political affiliation, they may so do. Such actions could lead to liability for the government official who employs this social media platform.

ADA Considerations

Local governments must comply with the Americans with Disabilities Act (ADA) and provide all individuals with equal access to programs, services and activities.[5] It is well settled that these requirements apply to local government and government officials' websites. It is not necessary to engage in an exhaustive discussion of what makes a website accessible or how to determine whether a website is accessible. The determination of whether a website or social media platform is ADA compliant is best accomplished by the City's Department of Information Technology (IT). IT routinely examines social media platforms for ADA compliance.

Wisconsin Open Meetings Laws

The Wisconsin Open Meetings Laws (OML) apply anytime that a sufficient number of members of a public body gather (concurrently or serially) and conduct the business of that body. Conducting public business is not limited to taking action on agenda items, but also includes information gathering and deliberating. The OML applies regardless of whether such gatherings occur in-person, on the telephone or in a more virtual context such as instant messaging, text messaging, chat rooms or social media platforms. See, for example, the discussion in the City Attorney Formal Opinion 2004-001 on the possibility of email constituting an illegal meeting. (http://www.cityofmadison.com/attorney/documents/2004opinions/2004-001.pdf). The risk is much greater with more interactive social media.

5 Unless doing so would fundamentally alter the nature of the programs, services or activities or would impose an undue burden upon the local government.

At its core the OML requires a minimum of 24 hours' notice of a meeting, the publication of an agenda and the conduct of meetings in publicly accessible locations. It may be difficult, if not impossible, to comply with the OML when using social media platforms.

Alderpersons should review §2.15, MGO, which is one of the Standing Rules For The Government of the Common Council. That rule places greater restrictions on the ability to utilize social media for Common Council meetings than does the OML. Under that rule no council member may vote by proxy nor may a meeting be held either telephonically or electronically unless it is a special or emergency meeting. Furthermore, that rule states "[n]o member of the Council shall communicate electronically with another member of the Council during a meeting on any matter in the meeting agenda, unless the electronic communication is saved and available under the Public Records Law and unless such communication in no way violates the Open Meetings Law."

Wisconsin Public Records Law Requirements

Content posted to a government official's professional website qualifies as a "record" under the Wisconsin Public Records Laws (PRL). Therefore, such content is presumed open to public inspection and must be archived in accordance with the City's records retention schedule. That schedule requires the archiving of such records for a period of three years beyond their creation. We are unaware of any social media platform that assists government officials in properly archiving their social media content and in making such content available for public inspection. Social media platforms have their independent and varied archiving policies, some don't even archive content. If a social media platform is bought out or ceases to exist, the government official may have no access to their records and no recourse to obtain them from the operators of the platform.

Against this background, the City's IT Department has developed and implemented procedures for archiving all approved City social media accounts. IT is available to assist government officials in responding to public records requests for access to their social media account contents, provided that the official is using a platform approved by the IT Department. IT may be unable to assist with the recovery of content that they were unaware existed.

TOS Issues

Many social media platforms apparently hope that people just click through the terms of service (TOS) when joining their platform. Seemingly nobody ever reads these lengthy and complex, often draconian legalese filled writings. However, clicking through these terms and using the software or website creates a contractual relationship between the user and the social media platform.

These documents often contain clauses requiring the user to hold the website harmless for any losses or damages occasioned by the use of the website. They may commit the user to user to resolving claims through binding arbitration. They often contain damage limits, choice of laws and

choice of venue designations[6]. Many of the standard terms are inconsistent with or diametrically opposed to the contracting terms that the City may lawfully accept.

The federal government has negotiated government compatible TOS with many social media platforms[7]. Wherever possible, the City prefers use of a platform with federally approved TOS to one without federally approved TOS. APM 3-20, Software Acquisition Policy, requires the approval of IT prior to accepting any TOS for software, including the use of social media platforms. APM 3-16, Social Media And Department Websites Policy, requires consultation prior to the use or implementation of social media. The Common Council Social Media Policy states that the IT Department is the lead agency for all Common Council use of social media. Furthermore, that policy states that the IT Director will maintain a list of social media tools approved for Common Council usage and that the City Attorney will review each proposed use of social media for any lurking legal issues.

Emerging Privacy Laws

Personally identifiable information (PII) is any information coupled with a person's name that allows the identification of a specific person. Examples of PII include dates of birth, driver's license numbers, social security numbers, passwords and account numbers. Most states and the federal government have laws requiring notification to the consumer any time that a PII database has been breached. However, both the European Union[8] and the State of California[9] have enacted broad, sweeping data privacy laws that impose data storage and security obligations, upfront disclosures as to what PII is being gathered and for what purpose, the opportunity to "opt out" from PII storage, defined PII storage procedures and penalties hereto unheard of in the data security field. Both sets of laws are aimed at protecting the personally identifiable information of their constituents and providing remedies for breaches of data security. These protections may extend to wherever their constituents conduct their online business, regardless of where their constituents may be at the time of the transaction or where the website they are using is actually and physically located.

While these laws currently impose duties and liabilities upon e-commerce operators, the wholesale breaches of PII databases that are the genesis of such laws have not been limited to e-commerce merchants. Government agencies and officials have had data security lapses as well. Therefore, it is reasonable to expect expansion of these laws or the enactment of similar laws, to encompass government and government official's databases. We may be only one critical incident or one political candidate[10], away from broader applications of these laws.

---

6 See https://en.wikipedia.org/wiki/Terms_of_service (last accessed April 29, 2019) for a good discussion of Terms of Service.

7 See https://digital.gov/resources/federal-compatible-terms-of-service-agreements/ last accessed April 29, 2019.

8 Regulation 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) 2016 O.J.L. 119/1 [hereinafter GDPR].

9 California Consumer Privacy Act of 2018, Cal. Civ. Code §1798.100 [hereinafter CCPR].

10 Sem. Elizabeth Warren, a 2020 Presidential candidate, advocates the imprisonment of CEO's whose negligent supervision of their company leads to a massive consumer data breach. See

Compliance with these data privacy laws is beyond the scope of this memorandum. The point to be understood here is that data security is a matter of serious concern for any internet based activity. It is an issue that the IT Department and the Office of the City Attorney will continue to monitor and will consider with regards to the proposed use of any social media platform.

Ethics Ordinance

State and City Ethics laws also limit use of social media in some limited circumstances. For example, government resources are not to be used for campaign purposes, sec. 3.35(5)(b) and 3.35(8), MGO, strictly limit the use of city facilities to city uses. Thus, something seemingly as minor as linking a campaign blog or website to your city website likely is a violation of the Ethics Code. Similar prohibitions apply under State law.

Conclusion

Social media can be a powerful tool for rapidly communicating to a broad audience. As with any powerful tool, care and consideration should be given to its proper deployment. While personal use of social media rarely involves consideration of any legal issues, use of social media by government officials is fraught with such considerations. The City of Madison's social media policies (both APM's and the Common Council's policies) reflect careful consideration and reasoned application of the laws that apply to governmental use of these communication platforms. City of Madison employees and officials must acquaint themselves with and observe these policies.

https://slate.com/technology/2019/04/elizabeth-warren-equifax-cambridge-analytica-regulation-data-privacy.html last accessed 4/29/2019.