



ISSN 1935-0007

Cite as: 2014 (11) AELE Mo. L. J. 201

Employment Law Section – November 2014

Online Networking, Texting and Blogging by Peace Officers Part Two – Limitations on Management’s Right to Monitor Content

- **Introduction**
- **Political Content**
- **Collective Bargaining and Protected Activity**
- **Privacy and Passwords**
- **Attorney-Client Privilege**
- **Discriminatory Enforcement**
- **Anonymity**
- **Suggestions to Consider**
- **Resources and References**

This is Part 2 of a two-part article. To read Part 1, click [here](#).

❖ Introduction

Use of the Internet, including online networking sites, sometimes called social media, texting on various electronic devices such as smartphones and tablets, and blogging in various forms have all become increasingly ubiquitous. Law enforcement personnel, like everyone else, participate in such activities during their off-duty hours, and in many instances, while on duty too. This raises a variety of legal, and personnel issues for departments and agencies.

[Part One](#) of this two-part article addressed courtroom impeachment problems, policy implications and First Amendment considerations. Part Two discusses the limitations on management’s right to monitor the content of networking sites, blogs, and text messages. Particular aspects addressed include political content, collective bargaining and protected activity, privacy and passwords, attorney-client privilege in such communications, the possibility of discriminatory enforcement of employer rules, online anonymity, and some suggestions to consider. At the end of the article are some useful and relevant resources and

references. The resources and reference at the end of Part 2 should be read in conjunction with those listed at the end of Part 1.

❖ **Political Content**

While Part 1 of this article explored First Amendment issues and analysis in more detail, one subsequently decided case in this area is worth noting. In [*Bland v. Roberts*](#), #12-1671, 730 F.3d 368 (4th Cir. 2013), former employees sued the sheriff in his individual and official capacities, alleging that their termination violated their First Amendment rights to free speech and association.

During a political campaign deputies “liked” the sheriff’s political opponent’s Facebook page, among other actions. The trial found that merely “liking” a Facebook page was insufficient speech to merit First Amendment constitutional protection. The court distinguished the act of “liking” a page from actually posting more substantive comments on a page, which would be protected.

The appeals court found that two former sheriff’s office employees presented First Amendment free expression claims that could withstand summary judgment because their support for the sheriff’s opposition by their Facebook comment postings constituted protected political speech, and the sheriff had allegedly threatened employees with termination for such actions. At the same time, the court found that the sheriff personally was entitled to qualified immunity because a reasonable sheriff at the time could reasonably have believed that he was authorized to terminate his deputies for political reasons.

❖ **Collective Bargaining and Protected Activity**

One limitation on management’s ability to monitor employees’ online content may be labor laws which protect union activity, collective bargaining, and related protected activity. Such laws will currently vary greatly from state to state.

In [*Detroit Police Dept., and Detroit P.O.A.*](#), #C04A-001, 19 MPER 15, 19 MPER P15; 2006 MI ERC Lexis 94 (2006), the Michigan Employment Relations Commission found that management committed an unfair labor practice by suspending, with pay, a police officer who hosted a website that was critical to management.

The case involved a Detroit police officer who created a website with his own funds and managed it while off duty. The website, firejerryo.com, provided a forum for Detroit police

officers to express their concerns over issues within the department. It also provided a source of information to the community concerning issues within the department.

The website contained a guest book that permitted visitors to register their gripes. It had pages with satire and caricatures. The chief suspended the plaintiff, initially with pay, until he dismantled the site. The chief claimed the site contained racial slurs that were detrimental to the department. The officer was then suspended without pay, when he continued to operate the site.

The union filed an unfair labor practice charge, alleging that the city violated state labor laws by directing officer to shut down his website and by suspending him when he failed to do so.

An Administrative law Judge found that operation of the website was ‘protected concerted activity because matters addressed on the website included work-related subjects such as wages, promotions, manpower, and discipline, even though subjects unrelated to working conditions also appeared.

On appeal, the city claimed that some statements posted on the website constituted sexual harassment, or were racist in nature, or otherwise offensive. The Michigan Employment Relations Commission noted that there was no evidence that the officer posted these statements.

The Commission held that the city’s demand that the officer shut down his entire website, and the disciplinary action imposed, “constituted a violation of [the officer’s] rights under [state labor laws] to engage in protected concerted activity. We will not allow the suppression of ... protected speech simply because it occurs in conjunction with speech that is not protected by [state law], where there has been no showing of actual harm or adverse impact flowing from that speech.”

What is unusual is the way the issue was litigated. Normally it would be a judicial review from a civil service board, or a First Amendment lawsuit filed in state or federal court. The protected speech in this case was related to concerted activity by a member of the bargaining unit.

Subjects for collective bargaining are divided into those that are mandatory because they impact changes in working terms and conditions, those that are prohibited because they relate to core management prerogatives which are essential to carrying out the employer’s business or purpose, and permissive subjects of bargaining, which the union and employer can either agree to bargain about or which one party can refuse to bargain about, which does not fall within either of the two prior categories.

In [*Treas. Dept., I.R.S. and N.T.E.U. L-36*](#), #CH-CA-70509, 1998 FLRA Lexis 194, 1998 ALJ Dec 137, it was ruled that management could not prohibit employees sending personal e-mail without bargaining with the union. The new rule was a change in working conditions, and therefore required bargaining

The key here was that, for almost a full ten years after e-mail was first introduced for employees, e-mail was used by employees for both official business and nonofficial purposes without the employer challenging any personal use. “Furthermore, Respondent [the employer] was undeniably aware of the nonofficial E-mail usage since the record clearly disclosed that managers not only received nonofficial E-mail from bargaining unit employees without challenging the practice for several years, but managers and supervisors actually sent out their own nonofficial E-mail messages.”

- Had a strict policy been established at the beginning prohibiting the use of email on the employer’s computers to send or receive personal e-mail, the result may have been different.

❖ Privacy and Passwords

Another major restriction on a department or agency monitoring employees’ online content may be the right of privacy. In a growing number of instances, states have enacted laws protecting employees’ online privacy. A hot topic in this arena is the question of whether an employer can demand that an employee hand over their password to online accounts, such as Facebook, facilitating the monitoring of content, as privacy settings may otherwise limit access to some or all of the material.

California in 2013 enacted a law making it unlawful for employers to request employee or applicant user names and passwords to social media sites like Facebook and Twitter. Under the statute, there is no exception for law enforcement, but there are exceptions for the use of employer provided devices (as opposed to personal cell phones, computer tablets, etc.) and when the information is relevant to an investigation of employee misconduct. Access is also, of course, available under normal Fourth Amendment rules in connection with a criminal investigation. Similar laws are also in effect in Delaware, Illinois, Maryland, Michigan, and New Jersey. The National Conference of State Legislatures has a [webpage](#) that tracks such legislation.

A very important decision in the area of privacy and text messages is [*City of Ontario v. Quon*](#), #08–1332, 560 U.S. 746 (2010), in which the U.S. Supreme Court upheld the search of a police officer’s text messages on a government-owned pager. A warrantless review of the officer’s pager transcript was reasonable because it was motivated by a legitimate

work-related purpose, and was not excessive in scope. A separate detailed article on this case was previously published in this journal. See [The City of Ontario v. Quon Supreme Court Decision](#), 2010 (9) AELE Mo. L. J. 501.

❖ **Attorney-Client Privilege**

One subject that has come up is that of attorney-client privilege and confidentiality in connection with the content of text messages, emails, and other electronic communications between an employee and their lawyer, regardless of whether sent or received on a department owned or privately owned electronic device.

In [Stengart v. Loving Care Agency, Inc.](#), 201 N.J. 300 (2010), a private employer's regulations notifying employees that they had no expectation of privacy for the use of workplace computers did not convert an employee's e-mails with her attorney, sent through the employee's personal, password-protected, web-based email account into the employer's property. The attorney-client privilege outweighs an employer's unilaterally imposed privacy regulations. The court rejected the employer's claimed right to rummage through and retain the employee's emails to her attorney. Further, the employer's policy failed to warn employees that the contents of personal, web-based e-mails were stored on a hard drive and could be forensically retrieved and read.

The privilege of confidentiality can be lost, however, when the person themselves discloses the content of the communication to third parties. In [Lenz v. Universal Music](#), #5:07-cv-03783, 2010 WL 4789099, 2010 U.S. Dist. Lexis 125874, PACER Doc. 351 (N.D. Cal.), for instance, a federal court upheld a magistrate's decision to compel disclosure of attorney-client communications because the plaintiff had discussed the communications in e-mails and instant chats with her family and friends, in blog postings, and with the media.

Also see [Curto v. Medical World Comm.](#), #03CV6327, 783 F. Supp. 2d 373 (E.D.N.Y. 2011), in which a federal court initially ruled that an employee had a reasonable expectation of privacy that management would not reconstruct and access e-mails sent to and received from her attorney on her employer-provided laptop. Attorney-client privilege overrode the employer's policy allowing search and retrieval of documents from computers provided to employees. Ultimately, however, the court found that the defendants' objections to the order finding the employee's communications privileged were moot because the plaintiff had waived the privilege by voluntarily disclosing the communications during discovery.

❖ Discriminatory Enforcement

One restriction on management's ability to monitor the content of personnel's use of online social media is that whatever rules are promulgated and enforced must not be handled in a discriminatory manner. Rules must be evenly enforced, not selectively enforced on the basis of race, religion, sex, age, disability, or other categories of people protected by federal, state, or local law.

In [*Hanners v. Trent*](#), #11-1754, 674 F.3d 683, 114 Fair Empl. Prac. Cas. (BNA) 965 (7th Cir. 2012), a Caucasian state police sergeant used his agency's official email system to send "humorous" descriptions of fictitious Barbie Dolls to fellow officers. Each fictitious doll was a caricature of a stereotypical woman living in an identifiable area in and around the state capitol. He was disciplined for this action, suspended for thirty days, and suffered the lowering of his promotion rating. He sued, claiming that he was subjected to race discrimination.

Rejecting this claim, a federal appeals court found that the plaintiff failed to show that non-Caucasians had been treated differently for similar conduct. There was absolutely no evidence of any discriminatory attitude towards him for being Caucasian. His argument that, had he been an African American he would not have been suspended for 30 days was pure speculation. While no discrimination was found in this instance, the implications of the court's reasoning are clear.

❖ Anonymity

Many available online forms of communications allow persons to engage in either completely anonymous communications or the use of a pseudonym or pen name. In some cases, courts have been protective of such anonymity. Clearly, to the extent that communication is anonymous, it is extremely difficult to monitor an employee's online content.

In [*Krinsky v. Doe 6*](#), #H030767, 159 Cal. App. 4th 1154, 72 Cal. Rptr. 3d 231, 2008 Cal. App. Lexis 180, 36 Media L. Rep. (BNA) 1321, for instance, a California appellate panel rejected an attempt to learn the identity of an e-message board user that disparaged another person. "The use of a pseudonymous screen name offers a safe outlet for the user to experiment with novel ideas, express unorthodox political views, or criticize corporate or individual behavior without fear of intimidation or reprisal. In addition, by concealing speakers' identities, the online forum allows individuals of any economic, political, or social status to be heard without suppression or other intervention by the media or more powerful figures in the field."

❖ **Suggestions to Consider**

Every department, agency, or facility should have a detailed, written, and well-publicized policy on employee use of both department-provided electronic devices and employee's use of social media, text messaging, and blogs.

Here are some suggestions to consider:

1. Inform employees that any and all communications sent or received using employer provided devices are subject to monitoring and that they have no reasonable expectation of privacy for any such communications.
2. A good policy will regulate the content of employee communications on social media, in text messages or email, or on blogs, insofar as a person is identified on the website or in the communication as an employee, since such communications represent and reflect on the department and its reputation and image in the community.
3. Law enforcement agencies should require that in blogs, social media or other forms on online communication that relate to the department or the city, or issues or activities in which the department is engaged, department employees should use their accurate identity, rather than communicating anonymously.
4. Social media provides a new and potentially valuable means of assisting the department and its personnel in meeting community outreach, problem solving, investigative, crime prevention, and related objectives.
5. Employees have a right to have personal web pages or sites. When reference is made to or about the department or agency, a review of that reference is needed to ensure that it does not compromise the employer's integrity or undercut the public's confidence in law enforcement.
6. Express written permission should be required before posting, transmitting and/or disseminating any photographs, video or audio recordings, likenesses or images of department logos, emblems, uniforms, badges, patches, marked vehicles, equipment, or other material that specifically identifies the department or agency.
7. Photographs of the inside of police buildings as well as any crime or accident scene shall not be posted.
8. If an employee indicates in any public forum any opinion on a law enforcement-related issue, then that employee shall state that the views and opinions expressed are their personal ones, and not those of their employer.

9. Employees should consider the possible adverse consequences of internet postings, such as future employment, cross-examination in criminal cases, and public as well as private embarrassment.

❖ Resources

The following are some useful resources related to the subject of this article.

- [Collective Bargaining - Duty to Bargain](#). AELE Case Summaries
- [E-Mail/Internet - Legal Issues](#). AELE Case Summaries
- [Privacy Rights](#). AELE Case Summaries
- [Specimen Law Enforcement Social Networking Policies](#)

❖ Prior Relevant Monthly Law Journal Articles

- [Bulletin Boards](#), 2010 (6) AELE Mo. L. J. 201.
- [Online Networking, Texting and Blogging by Peace Officers Part One – Impeachment, Policy & First Amendment Issues](#), 2010 (4) AELE Mo. L. J. 201.
- [The City of Ontario v. Quon Supreme Court Decision](#), 2010 (9) AELE Mo. L. J. 501.
- [The Use of Personally-Owned Mobile Phone Cameras and Pocket Video Cameras by Public Safety Personnel](#), 2012 (2) AELE Mo. L. J. 501.

❖ References

- [Electronic Privacy and Employee Speech](#), by Pauline T. Kim, Chicago-Kent Law Review (2012).
- [Officer's personal cell phones – Subject to discovery?](#) by Martin J. Mayer, presented at the International Association of Chiefs of Police 2011 Annual Conference, Chicago, Illinois.
- [Social Networking in Law Enforcement](#), by Martha Stonebrook and Rick Stubbs, presented at the International Association of Chiefs of Police 2010 Annual Conference, Orlando, Florida.

- [Employment Issues Related to Electronic Communications](#), by Jody Litchford, presented at the International Association of Chiefs of Police 2009 Annual Conference, Denver, Colorado.
 - [When Does an Employer's Search of Employee Work Areas Violate Privacy Rights?](#) Police Chief (Aug. 2008).
 - [Instant and text messaging report](#) by the National Assn. of State Chief Information Officers, "The Privacy Implications of Instant and Text Messaging Technologies in State Government" (2005).
 - E-mail, fingerprints and personnel files: Recurring and emerging discovery issues in employment litigation, 38 (1) Tort Trial & Insur. Prac. Law Journal 69-101 (Fall 2002), Amer. Bar Assn.
-

AELE Monthly Law Journal

Bernard J. Farber
Employment Law Editor
P.O. Box 75401
Chicago, IL 60675-5401 USA
E-mail: bernfarber@aele.org
Tel. 1-800-763-2802

© 2014, by the AELE Law Enforcement Legal Center

**Readers may download, store, print, copy or share this article,
but it may not be republished for commercial purposes. Other
web sites are welcome to link to this article.**

- The purpose of this publication is to provide short articles to acquaint the reader with selected case law on a topic. Articles are typically six to ten pages long. Because of the brevity, the discussion cannot cover every aspect of a subject.
 - The law sometimes differs between federal circuits, between states, and sometimes between appellate districts in the same state. AELE Law Journal articles should not be considered as "legal advice." Lawyers often disagree as to the meaning of a case or its application to a set of facts.
-

[AELE Home Page](#) --- [Publications Menu](#) --- [Seminar Information](#)

This article appears in the [IACP Net](#) database.