

**The Bill Blackwood  
Law Enforcement Management Institute of Texas**

---

---

**The Management Challenges of Social Media for  
Law Enforcement Employees**

---

---

**A Leadership White Paper  
Submitted in Partial Fulfillment  
Required for Graduation from the  
Leadership Command College**

---

---

**By  
James C. Summitt**

**Denton Police Department  
Denton, TX  
May 2016**

## **ABSTRACT**

This paper addresses the problems facing public employers with special emphasis on law enforcement agencies regarding employee use of social networking sites off duty. There is ample documentation of public employees impeaching their personal credibility as well as their employer's reputation as a result of the content posted onto social networking sites. This paper is a literary review of print and online media articles, case law, and peer reviewed journals specific to this topic.

The world is shrinking and the electronic community has emerged as a substantial and legitimate force. People conduct commerce, receive education, and carry on relationships through electronic forums. Social networking is a major aspect of modern American life. Public employers should proactively take steps to address the content of their employee's social networking sites. However, employers seem to view social networking sites as a gray area. The employer extends privacy protections and free speech protections where they are inappropriate.

This research clarifies the privacy issues and free speech issues concerning an employee's off duty conduct in the world of social media. It documents the legitimacy of electronic communities. It also addresses the employer's right to regulate off duty conduct. The last major theme concerns the construction and need for a well thought out policy governing the use of social media by public employees. The paper concludes that agencies should enforce off duty code of conduct standards on content posted on social media sites.

# TABLE OF CONTENTS

	Page
Abstract	
Introduction . . . . .	1
Position . . . . .	4
Counter Position . . . . .	8
Recommendation . . . . .	11
References . . . . .	14

## INTRODUCTION

Technology usually presents some growing pains as people enjoy new conveniences as well as discover new problems. Social media networking websites such as Facebook, Myspace, and Twitter affirm this position. The convenience of connecting and maintaining long distance friendships is a benefit to maintaining a social networking website. However, there has been an unforeseen consequence. People are sharing intimate details and making off color remarks as if they were engaged in a private conversation. The conversations have consistently proven to not be private. The off color remarks are not simply forgotten. They are memorialized in cyberspace, often for unintended eyes to see. The spillover hits full force when people *friend* their coworkers, making people in their workgroups privy to these comments.

The growing pains of social networking play out consistently in newspaper headlines across the country. The end result of poor conduct memorialized in cyberspace can be termination from employment. This has proven true for public employees, be they teachers, elected officials, or police officers.

Dwyer (2010) published an article on a law enforcement professional website detailing the potential problems social networking poses to police officers. The article discusses several problems agencies may face when dealing with misconduct that is displayed on social networking websites. These problems may include the muddy waters of an employee's right to free speech while off duty versus the agency's need to protect its professional image. There are also generational factors at play. Many police executives have little experience with social networking media while many new officers are dependent on the social outlet it provides. The article documents well publicized

incidents of officer testimony being impeached in court due to inappropriate remarks memorialized on their social networking website. The article also documents some problems that overseas police agencies are facing due to employee misconduct documented on a social networking site.

An internet search produced several other and lesser known instances of officer misconduct connected to social networking sites. An officer was fired in Moncks Corner, South Carolina, due to photographs published on Facebook by a third party. The officer took his marked patrol unit to a charity carwash where women in bikinis posed for pictures while washing the car. The business sponsoring the car wash published pictures on their Facebook page. The officer lost his job as a result of the incident. The city did not like its police department associated with a bikini car wash. Interestingly, one of the bikini clad women was an off duty sheriff deputy. She received no disciplinary action for the photograph or her participation since she did not represent herself as an employee of the sheriff department during the event (MacDougall, 2010). A Sandy Springs, New Jersey, officer was fired for publishing sensitive work related information on his Facebook page. The officer erroneously assumed that the postings intended for friends would not become available for public consumption (Stevens, 2009). Another officer in New Jersey was suspended for making inappropriate remarks on Facebook about a prominent religious member of the community (Johnson, 2010).

These instances drive home the need to enforce department code of conduct standards on social networking sites. The law enforcement industry has not been caught completely unaware. The International Association of Chiefs of Police (2010) has released a model policy for regulating employee social networking sites. The policy

allows for professional use of social networking sites by the agency as an entity. It also addresses standards of conduct by employees with caveats on making specific job references, engaging in speech directed specifically to circumstances at work, the safety issues of revealing too much personal information in an online forum, and the lack of privacy with respect to social networking sites. There is also a formal warning that employees will be accountable for the information they post onto their social networking site.

Enforcing department conduct standards on social networking sites is a gray area solely due to unfamiliarity resultant from the relative newness of the widespread use of social networking sites. Law enforcement managers should proactively enforce department conduct standards for conduct occurring in cyberspace on social networking sites. There is strong precedent for this practice. Courts have recognized an agency's need to protect its professional image in the community. There is significant case law supporting an agency in regulating the off duty conduct of its employees. Finally, cyberspace and social networking sites have been mislabeled as *virtual communities*. The label implies that the friendships, interactions, and consequences are somehow not real. These communities are real and the relationships can be significant. The counterarguments to not regulating social networking conduct are flimsy or misguided. Administrators are willing to extend free speech protections where they are not warranted. Managers may tolerate misconduct to establish the concept of off time by disengaging from *virtual* misconduct. This disengagement is centered on respecting employee privacy away from work in a venue that is anything but private.

## POSITION

The first challenge in addressing how officers use social networking is realizing the legitimacy of the virtual community as an actual community. By labeling a community as virtual, the idea is conveyed that the community is somehow less substantial. Law enforcement is primarily focused on geographic community concepts. This is evident in community policing philosophies as well as the spatial hotspot mapping concepts. Police managers need to understand the actual importance of virtual communities.

Technology is a major facet of most people's lives. E-commerce sales topped \$1 trillion dollars in 2012 (Hof, 2013). Electronic marketplaces like Amazon represent significant threats to traditional brick and mortar businesses. Education has also experienced a radical expansion of online learning. Sixty-five percent of university administrators see online education as an integral part of their institutions future plans, while 67% of educators rated online courses as equal to or superior to face to face instruction (Lytle, 2011). The International Association of Chiefs of Police conducted a survey in 2013 that reported that more than 95% of surveyed agencies using social media (IACP, 2013). It is clear that the virtual community is substantial in terms of peoples' commercial lives. Many law enforcement agencies use social media to engage their communities and investigate criminal offenses.

Nostalgic reminiscing of community still brings up images of a geographic neighborhood, a physical place where friends, commerce, and interests reside. Hampton and Wellman (2003) challenges this concept directly, claiming that people have more social ties outside of the geographic boundaries of their physical

neighborhood than inside it. They go on to state that communities exist outside physical boundaries and imposing physical boundaries ignores the social aspects of current communities. Wellman (2001) stated that people feel social support, companionship, and belonging from online interaction. These are identified as the criteria needed for strong communal ties. Access to social networking sites is ingrained in peoples' daily lives (Waring & Buchanan, 2010). This is painfully obvious as people have the ability to remain connected to these sites via a smartphone device throughout their entire day. The community has moved from the semi-public physical neighborhood to living rooms and handheld devices that allow access to the online communities where social needs are satisfied (Wellman, 2001).

Geographic communities remain important. Equally important is recognizing the legitimacy of the electronic community. People are spending money in electronic markets. They are in electronic classrooms. They are meeting their spouses online. Police departments are using social networking sites to interact with their communities and conduct investigations. Most importantly, police employees, like any other citizen, are participating in these online communities. These online communities are real. They must be viewed with equal importance when compared to physical communities.

Police departments have a well-established right to monitor the conduct of their employees while they are off duty. This is not *carte blanche* for the department as an employer to intrude into all aspects of their employees' lives. The department must demonstrate a provable connection between the employee's conduct and the ability of the employer to remain effective in its mission (Atchison, 2009). An excellent example of this premise is the case of *Roe v. San Diego* (2004). John Roe was employed as a

San Diego police officer. Roe earned money by selling sexually explicit video tapes of himself on eBay. Roe would dress in police costumes but not his official San Diego police uniform. Roe would identify himself as a police officer but not identify the actual agency that employed him. Roe did engage in selling actual San Diego PD uniform items on eBay under the same seller profile that he sold the sexually explicit videos. Roe's employer discovered Roe's activities and ordered him to stop. Roe failed to stop and was eventually fired for conduct unbecoming an officer, improper outside employment, and immoral conduct. Roe's termination was upheld 9-0 by the United States Supreme Court (*Roe v. San Diego*, 2004). Thus, Roe's employer was able to successfully argue the negative impact of Roe's behavior on its ability to carry out its mission. This is just one instance of many where police departments as employers had their right to regulate off duty conduct upheld.

Tyler (2006) reported that, "people that view police as legitimate are more likely to accept their decisions" (p. 379). Protecting the legitimate perception of authority is an important task to police administrators. Legitimate authority is the source of voluntary compliance in a population (Tyler, 2006). An attorney game planning for cross examination of police officers stated, "It is now a matter of professional competence for attorneys to take time to investigate social networking sites. You must pan for gold where the vein lies, and today the mother lode is often online" (Nelson, Simek, & Foltin, 2009, p. 12). This clearly indicates the potential for off duty conduct on a social networking site to impeach an officer's credibility in court. Thus, conduct on a social networking site has real implications for individual and departmental legitimacy within the community.

Regulating off duty conduct is done to protect an officer's effectiveness in carrying out their official duty (Woronoff, 1984). Courts have continually upheld an agency's right to regulate off duty behavior as central to protecting its legitimate authority. Police departments' ability to operate in communities is improved when their authority is perceived as legitimate making their officers entitled to receive community support and obedience (Tyler, 2006). Just as a department would regulate an off duty officer's choice to be obviously drunk in a bar in the community, the same department should regulate an officer documenting a night of debauchery on their social networking site.

As organizations adapt to the widespread use of social networking sites, they must establish sound policies moving forward. Questionable behavior that violates a poorly and subjectively constructed policy will result in public outrage (Woronoff, 1984). The ideal policy should promote agency needs while being minimally intrusive on the officer's ability to interact with friends. The International Association of Chiefs of Police has written a model policy that incorporates several desirable recommendations. An ideal policy should restrict the disclosure of employment and use of images containing department logos. It should explicitly connect the content of social networking sites to code of conduct expectations. The policy should explicitly limit an employee's ability to comment in any official capacity. And the policy should clearly state that speech by employees cannot be of such content that it would negatively impact the department (IACP, 2010).

It has been established that online communities are viable and real. Commerce is conducted, relationships are entered, maintained, and ended, professional

development and education occurs. It is within reason to believe that the destruction of a professional reputation can also occur. To protect from the destruction of personal and organizational reputations, departments need to establish code of conduct policies to guide employees on and off duty. These policies must extend into the online communities of social networking sites.

## **COUNTER POSITION**

There are two primary arguments against regulating employee's social networking site content. The first argument centers around an individual's right to free speech. The second argument centers around an individual's right to privacy.

The government as an employer is in a unique position. Sprague (2007) documented that most courts do not extend the right of free speech with respect to private employment. In other words, a private employer has no obligation to guarantee an employee's Constitutional Rights. However, the government as an employer is subject to the same Constitutional limitations imposed on it as a governor. Thus, the government as an employer must ensure constitutional protections for its employees. An employee posting non-work related issues on a social networking site off duty should expect to be left alone by their government employer (Secunda, 2009). This seems to be common sense. Some interpret the First Amendment as a license to say anything. The analogy that a person cannot yell fire in a crowded theater has been stated numerous times as a free speech limitation. The better concept would be that free speech does not mean speech is without consequence. Patrick Shearer of Peoria, Arizona police was demoted as a result of posting a photo of a T shirt with President Obama's face on it after the T-shirt and image had been shot numerous times at a gun

range (Thomas, 2012). Thus, Shearer was not clear that his right to engage free speech even of a political nature still had some limitation.

Clearly a public employee's right to protected free speech has limitations. The more an employee infuses work related topics that result in work disruptions, the more likely the employer will be able to successfully discipline an employee (Secunda, 2009). There is a difference between free speech and protected speech. Public employees have the potential to reveal information that is important to public discourse. This speech is protected. Case law has established criteria for determining what speech would be considered protected by the First Amendment. The specific criteria for determining if speech made by a public employee in their capacity as a private citizen is protected is as follows. First, the speech must address a matter of public concern. Second, the speech must be the primary factor for causing the employer to take a negative action against the employee. Third, the employee's interest as a citizen should be balanced against the employer's (government agency) interest in accomplishing its mission. These criteria are called the Pickering Test (*Pickering v. Board of Education*, 1968). Bettering the workplace could be an issue of public concern. Gripping over internal issues rarely is afforded Constitutional protection (Sprague, 2007). Further, the personal nature of posts to social networking sites make it difficult for them to qualify for first amendment protection (Secunda, 2009).

Examining the instance involving Shearer using the Pickering Test, Shearer clearly has a legitimate interest in making a complaint about the president. His employer demoting him was clearly motivated by his political statement. What allowed his employer to demote him was the balance between Shearer's right to speech versus

the agency's quest to be effective in its mission. Shearer's method of protest caused enough alarm with the United States Secret Service to compel an investigation. This clearly impacted the Peoria Police Department's reputation especially at a time when the president was planning to be in the area (Thomas, 2012, *Pickering v. Board of Education*, 1968). Therefore, in the balance element of the Pickering Test, the agency wins. These types of situations demonstrate the need for law enforcement employers to monitor social networking activities of its employees. This situation also demonstrates that both the employer and employee are limited in what they can and cannot do under the First Amendment.

Employees will also claim a right to privacy when confronted on their blog posts. The right to privacy, while not explicitly stated by the Constitution, is inferred through case law invoking the 1<sup>st</sup>, 3<sup>rd</sup>, 4<sup>th</sup>, 5<sup>th</sup>, and 9<sup>th</sup> Amendments. The right to privacy generally falls into two categories: an interest against being compelled to disclose personal matters or an interest in being let alone (Atchison, 2009). The ability to post onto a social networking site without intrusion will fall into a person's interest to be let alone.

Most of the controversy surrounding social networking hinges on whether or not your social networking site is truly private. The Facebook User Agreement (2013) states that users may use security settings to some effect, but most content becomes Facebooks' by way of its user agreement which allows them use it as they see fit. Thus, Facebook more or less owns whatever is posted there.

The right to privacy on a social networking site or any other type of blog is a myth. Social networking sites create an illusion of being able to control content, but the

reality is there is no mechanism or law to truly limit content (Gelman, 2009). Further, there are no federal laws prohibiting an employer from accessing an employee's social networking site page if the employee's security settings allow it (Genova, 2009). Privacy rights do not attach to information voluntarily shared in a public forum, and social networking sites are considered public forums (Timm & Duven, 2008). It is obvious that when an individual creates a social networking site page, they are willingly sharing personal information about themselves. Herbert (2009) pointed out several problems areas for public employees choosing to use social networking sites. The sites themselves are designed for exhibitionism. There is a disassociation between the content of what is posted and the potential for a disciplinary consequence. And there is a likelihood that an employee will allow access to a supervisor or other members of their work group who may share the content with a supervisor.

Thus, people willingly enter into user agreements with social networking sites that give control over personal information to others. All information that is shared is provided willingly to the social networking site. By definition, this is anything other than private. The concept of the right to privacy seems appropriate on a social networking site simply because of the volume of information posted there that should be private. The reality is that social networking sites are public forums, and law enforcement administrators should be confident in treating them as such.

## **RECOMMENDATION**

Technology has pushed the concept of the traditional geographic community. It has created an online community that is every bit as dynamic. More than a trillion dollars were spent in online stores in 2012 (Hof, 2013). The majority of universities factor

online education as a major facet of their future plans (Lytle, 2011). Social networking sites more than adequately facilitate personal and intense social interaction (Wellman, 2001). These online communities are powerful and real, which means that law enforcement administrators must know how to respond to them.

There is ample precedent for agencies to regulate the off duty conduct of their officers in the community. An agency's as well as the individual officer's reputation is impacted by poor conduct. Any police department would prefer that a member of its DWI task force not get publicly intoxicated in local bars. Likewise, the same agency would prefer that its officers not post intoxicated pictures of themselves in public or private areas of the community on social networking sites.

Officers will state that they have a right to free speech and a right to privacy. They will assert that their social networking site page is private due to the personal information stored there. They will also state that their security settings have established their intent to keep their page private. This is a flawed concept. One person may have their security settings set to prohibit anyone but a friend from seeing their content. However, an approved friend may have a wide open social networking site page exposing all of the posts or images involving them to anyone. Facebook's own security agreement states that other people and entities will potentially control content ("Facebook User Agreement," 2013). Thus, there is no privacy attached to these sites.

Free speech is a fundamental American right. It does not mean a person can say anything they want. It means there is very little speech for which a person can be sanctioned by the government. The Pickering Test clearly protects from consequence speech that is of public concern after being weighed against an individual's right to

engage in discourse on issues important to the public versus a government entity's need to function efficiently and effectively (*Pickering v. Board of Education*, 1968). This means that griping over policy issues, personality conflicts, or operational decisions most likely will have consequences. An increased frequency of terminations due to blogging activities is also predicted (Sprague, 2007).

Agencies need to confidently step into the arena of safeguarding their reputations from damage done in the realm of social networking communities. The best and most fair approach is to establish a policy of clear expectations and unacceptable behavior. Sprague (2007) states that "employers should have some type of social networking policy" (p. 7). Companies accessing social networking sites should have some type of policy in place (Genova, 2009). Waring and Buchanan (2010) recommends that employers be clear about how they intend to access and use employee social networking information.

The IACP (2010) model policy addresses acceptable behavior, the public nature of social networking sites, how employees attach themselves in this forum to their employer and many other aspects. It is not a one size fits all policy. This issue needs to be carefully assessed by each agency with policies drafted specifically to that agency. The clear consensus is that a law enforcement agency needs to have a policy establishing acceptable conduct for its employees engaged in the use of social networking sites, and it needs to be prepared to enforce its standards.

## REFERENCES

- Atchison, W. (2009). *The Rights of Law Enforcement Officers* (6<sup>th</sup> ed.). Portland, OR, LRIS.
- Dwyer, T. (2010, August 11). Pitfalls for police officers on Facebook. *PoliceOne.com*. Retrieved from <https://www.policeone.com/off-duty/articles/2304799-Pitfalls-for-police-officers-on-Facebook/>
- Facebook user agreement. (2013, November 15). Retrieved from <https://www.facebook.com/terms>
- Gelman, L. (2009). Privacy, free speech, and “blurry-edged” social networks. *Boston College Law Review*, 50(5), 1315-1344.
- Genova, G. (2009). No place to play: Current employee privacy rights in social networking sites. *Business Communication Quarterly*, 72(1), 97-100. doi: 10.1177/1080569908330377
- Hampton, K. & Wellman, B. (2003, December). Neighboring in netville: How the internet supports community and social capital in a wired suburb. *City and Community*, 2, 277-311. doi: 10.1046/j.1535-6841.2003.00057.x
- Herbert, W. (2010, June). Workplace consequences of electronic exhibitionism and voyeurism. Paper presented at the 2010 IEEE International Symposium on Technology and Society Social Implications of Emerging Technologies. Wollongong, New South Wales.
- Hof, R. (2013, February 5). You know what’s cool? A trillion dollars in e-commerce. Retrieved from <http://www.forbes.com/sites/roberthof/2013/02/05/you-know-whats-cool-a-trillion-dollars-in-e-commerce/>

International Association of Chiefs of Police. (2010). Model policy: Social media.

Alexandria, VA: Author.

International Association of Chiefs of Police. (2013). 2013 survey results. Alexandria,

VA: Author. Retrieved from

<http://www.iacpsocialmedia.org/Resources/Publications/2013SurveyResults.aspx>

Johnson, B. (2010, August 25). Cataret police union claims cops disciplined for

ticketing officials; mayor says reprimand was over inappropriate comments on

Facebook. *The Star Ledger*. Retrieved from

[http://www.nj.com/news/local/index.ssf/2010/08/carteret\\_police\\_union\\_claims\\_c.html](http://www.nj.com/news/local/index.ssf/2010/08/carteret_police_union_claims_c.html)

Lytle, R. (2011, November 11). Study: Online education continues growth. Retrieved

from [http://www.usnews.com/education/online-](http://www.usnews.com/education/online-education/articles/2011/11/11/study-online-education-continues-growth)

[education/articles/2011/11/11/study-online-education-continues-growth](http://www.usnews.com/education/online-education/articles/2011/11/11/study-online-education-continues-growth)

MacDougall, D. (2010, September 23). Deputy in bikini OK; sudsed-up patrol car, not

OK. *Charleston Post and Courier*. Retrieved from

<http://www.postandcourier.com/article/20100923/PC1602/309239880>

Nelson, S., Simek, J., & Foltin, J. (2009). The legal implications of social networking.

*Regent University Law Review*, 22(1), 1-30.

Pickering v. Board of Education, 391 US 563 (1968).

Roe v. San Diego, 543 US 77 (2004).

Secunda, P. (2009). Blogging while publicly employed: Some first amendment

implications. *University of Louisville Law Review*, 47(4), 1-18.

- Sprague, R. (2007, Winter). Fired for blogging: Are there protections for employees who blog? *University of Pennsylvania Journal of Labor and Employment Law*, 9(355), 1-30.
- Stevens, A. (2009, December 9). Officer: Facebook postings didn't warrant firing. *The Atlanta Journal Constitution*. Retrieved from <http://www.ajc.com/news/news/local/officer-facebook-postings-didnt-warrant-firing/nQZsF/>
- Thomas, J. (2012, February 28). Peoria police sergeant demoted over Obama photo on Facebook. Retrieved from <http://www.azfamily.com/story/28346171/peoria-police-sergeant-demoted-over-obama-photo-on-facebook>
- Timm, D. & Duven, C. (2008, Winter). Privacy and social networking sites. *New Directions for Student Services*, 124, 89-101. doi: 10.1002/22.297
- Tyler, T. (2006, July 8). Psychological perspectives on legitimacy and legitimation. *Annual Reviews Psychology*, 57, 375-400.  
doi:0.1146/annurev.psych57.102904.190038
- Waring, R. & Buchanan, F. (2010, Spring). Social networking web sites: The legal and ethical aspects of pre-employment screening and employee surveillance. *Journal of Human Resources Education*, 4(2), 14-23.
- Wellman, B. (2001, September 14). Computer networks as social networks. *Science*, 293(5537), 2031-2034.
- Woronoff, M. (1984). The off duty sexual activities of police officers and the constitutional right to privacy. *University of Michigan Journal of Law Reform*, 1-23.