The Bill Blackwood
Law Enforcement Management Institute of Texas

Using Education and Training to Avoid Pitfalls of Social Networking

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

By
Charles Kreidler

Texarkana Police Department
Texarkana, Texas
February 2011

ABSTRACT

The education of supervisors and officers in the use of social networking internet sites is an important issue for law enforcement agencies. The instances of officers being disciplined for on and off duty activity on these sites is evidence that action is required on the part of police executives concerned with the future. Law enforcement agencies should recognize the explosive growth and potential threat in the area of social networking sites and respond with a proactive approach of education and training with emphasis on existing department policies. The information used to support this recommended approach consisted of a review of standard management methods, published studies, periodicals and internet sites, including numerous print media archives. It is easy to say that a new policy will handle the issue; however, the key to success will be educating officers and supervisors on the common-sense use of these internet sites. Officers must be educated to the fact that some use of social networking can be detrimental to them personally and professionally.

TABLE OF CONTENTS

INTRODUCTION

During the past decade, there has been phenomenal growth in internet social networking, and at the top of the provider list is Facebook. Started by one college student as a way for other students to keep track of friends, the site continues to grow at a staggering pace. The Nielsen Company (Nielsen Netview, 2010) showed that the top social networking site in December 2009 was Facebook, with 206,878,000 individual users and an average use time per person of just less than six hours. Facebook was number four on the Nielsen top ten website usage list behind Google, Microsoft, and Yahoo. To put this into perspective, the average use time per person for Facebook is almost double that of all the others in the top ten for the same time period and includes those already mentioned as well as EBay and Amazon.

In order to better understand the proliferation of social networking into the mainstream, it is necessary to look at the growth in the number of Facebook users during the last half of the decade. The numbers taken from Facebook's statistical page showed that in 2006, there were 12 million active users; in 2007, there were 50 million; in 2008, there were 100 million; and, finally, at the end of 2009, there were 350 million active users (Facebook, 2010). There were three other figures found on the statistical page that illustrate one cause for concern to police agencies. The average user spends 55 minutes per day logged in, there are 2.5 billion photos uploaded to the site each month, and 65 million users access Facebook through mobile devices such as the iPhone. These numbers are staggering and should bring police executives to the realization that Facebook and other similar sites are permeating the daily lives of officers under their command.

In order to address the problems associated with these sites, police executives should first educate themselves on the pitfalls and hazards that are present. There are several studies, court cases, and other documented information that deal directly and indirectly with the use and problems associated with these types of internet sites. The studies reviewed for this paper deal with the human factors surrounding usage while the more recent news articles are glowing examples of the outcome of law enforcement officer's improper posting of material.

POSITION

The keys to preventing mistakes and to avoid violating department policy in the use of social networking will be the education and training of police officers in acceptable use. As studies showed, there is a lack of knowledge on the part of the users when dealing with privacy issues and reliance on the individual provider's privacy settings. The individual user plays a pivotal role in what information they share and it is the responsibility of law enforcement executives to ensure that officers understand the dangers.

Starting with the human factors, according to Lipford, Besmer, and Watson (2008), some of the major issues in using social networking are identity theft, stalking, embarrassment, and blackmail. Each of these has one common theme that should be the top concern for everyone, including police officers, and that is privacy. The posting of private information is tantamount to putting it on a billboard for everyone to see. For evidence of this one, only needs to review the Facebook privacy page where warnings are found that cover privacy issues. Under the heading of risks inherent in sharing information are statements such as "please be aware that no security measures are

perfect" and "We cannot ensure that information you share….will not become publicly available" (Facebook, 2010, How We Protect Information, para. 3). This, of course, is found in the fine print that most people do not give enough attention to.

A study by Acquisti and Gross (2006) on the awareness of privacy issues on Facebook revealed that 30% of respondents did not even know that Facebook had privacy controls. There should be more concern on the part of the user to ensure that personal information does not become public since social networking sites make no guarantees and advertise that their security measures are not perfect. An earlier study by Gross and Acquisti (2005) of over 4000 Carnegie Mellon University students showed, by large; that the participants in a study of social networking sites were oblivious and unconcerned about privacy. This would tend to show that even though the privacy warning is there for anyone to read, it is not necessarily a concern. The later study by Acquisti and Gross (2006) also suggested that privacy issues had some effect on the participants joining a social networking site, but, once a member, there was very little difference in the personal information shared by the user. A portion of this study also revealed that the posting of personal information may be a result of "peer pressure" or a "herding behavior."

Even with the website warnings with posting private information, individual users continue to put their personal information in an unsecured environment. It could be the result of the same peer pressure and herding behavior that Acquisti and Gross (2006) referred to, especially when one considers the volume of users previously mentioned. The user must struggle with the fact that their friends and co-workers are doing it, and they are expected to follow. It is possible that users are weighing the risks and placing

trust in the privacy settings of the individual website they are using. According to Dwyer, Hiltz, and Passerini (2007), there is a connection to what information is shared based on trust and usage goals of the individual user. In short, the intended benefits outweigh what is perceived as a minimal risk to privacy. While there is no definitive study on coupling the peer pressure and trust elements, it would stand to reason that there is a possibility of amplifying one or both when combined.

With regard to the disclosure of personal information, it can be determined from these studies that there are usage issues that include the factors of risk and trust. There is further research dealing with risk that shows the negative outcomes being outweighed by the benefits. A study of consumer disclosure found that participant's release of personal information was affected by the depth of relationship (White, 2004). The deeper the relationship, the more information released. If one considers the fact that Facebook users are inviting "friends" to view their posted content, one could say that the relationship is deep. The depth of this type of relationship would result in the perceived risks in release of personal information being outweighed by the potential benefits of communicating on a regular basis with "friends."

If the privacy issues were solved with a guarantee of security, there still has to be a common sense approach to what the individual user is posting and the trust being placed in system. The content of what a person posts could be just as harmful, personally and professionally, in the hands of someone the individual has authorized to view it, such as a "friend" on Facebook. A person may find that their "friends" would be the first to report or discuss with others an offensive comment or photo. In a survey by Cranor, Reagle, and Ackerman (1999), respondents cited trust as major factor in the

release of personal information to internet entities. With the amount of information being provided to Facebook and similar sites, it would seem there is a level of trust that has been placed in the provider and the user's individual "friends" that needs to be evaluated in light of recent law enforcement personnel issues.

In a review of current media reports, it is obvious that a firestorm can be created by a simple posting by an officer on a social networking site. Stevens (2009) reported the firing of a Sandy Springs, Georgia officer for his postings on Facebook. The officer in question posted comments about his upcoming work with the FBI on a possible drug sting operation. The officer claimed that his privacy settings only allowed his "friends" to view the content, but, ultimately, the information was made public. This particular incident highlights the previously mentioned areas of trust and risk along with a belief in security that is not infallible.

A different type of posting reported by Horton (2009) in Washington State described an officer in the final stages of training to be a Washington state trooper who was seen on Facebook in uniform and posing next to his marked cruiser. This alone may not be seen as problem. However, along with that photo were others depicting the trooper drinking from a pitcher of beer with comments about being intoxicated. Again, even though the officer had his privacy settings for friends and family, the information leaked out into the public. The officer was given the opportunity to resign after an investigation revealed what the state patrol regarded as "questionable activity."

An officer with the New Bedford Police Department in Massachusetts posted a photo allegedly depicting a dead body at the scene of a police investigation (Fraga, 2010). According to the agency, the action violated established department policy. New

Bedford also suspended an officer in 2009 for posting a photo of himself while in uniform on the relationship section of Craigslist. While these incidents are different in what was posted and for the intended audiences, they are similar in that both show a lack of common sense on the part of the officers making the posting. An officer educated in the hazards of social networking may have made a better decision.

From these examples found in the media, it is clear that officers are using social networking sites in the same manner as most other individuals. While in some cases they are posting confidential material that is accessible only because of their profession, they are doing so without regard for the fallout that could occur. It goes back to trust, usage goals, peer pressure, and lack of training and education.

The clear objective should be to educate the officers and stress the fact that they are held to a higher standard by the public, and they will garner more scrutiny than an ordinary citizen. There is no official study on the reasons, but one could surmise that the scrutiny is the reason the information is reported or made public by some acquaintance that the officer may think they could trust. Police agencies and the public, including "friends," expect law enforcement officers to behave in a manner that does not bring discredit upon them or the agency.

It would be easy to say that the best way to handle social networking would be to develop a comprehensive policy prohibiting activity on these sites. However, the very nature of personal use and the fact that the activity, in many cases, takes place off duty makes the monitoring of a policy problematic. Couple this with the low probability of detection, and the issue becomes an inability to effectively monitor the activity to ensure compliance, making the policy itself detriment. Evidence of this can be found in a study

conducted by Tenbrunsel and Messick (1999) in which compliance with policy was achieved in 76% of the participants when there were no sanctions or monitoring present. Compliance decreased to only 44% when there were weak sanctions and a low detection probability. This study is an example of the situation law enforcement faces with the off duty use of social networking and the inability to effectively monitor activity. Another interesting finding in the Tenbrunsel and Messick (1999) study was the fact that 80% of the participants selected the reasoning of “business decision” rather than an “ethical decision” in the situations where detection is unlikely due to weak monitoring. Thus the decision to follow a policy or directive as a business decision becomes a question of risk which, in the case of social networking sites, could be reduced with proper education.

The way to avoid the problems associated with sanctioning and monitoring a new policy would be to utilize existing policies already in place. In the absence of existing policies, police agencies would need to incorporate social networking into a new directive. However, if current policies exist that prohibit the release of information or prohibit personal business while on duty they could be incorporated into the education of officers on their use of social networking. Policies that prohibit conduct that brings discredit upon the officer of the agency could also be utilized. An example would be an officer seen by witnesses to be intoxicated in a public place is no different than a photo depicting the same being published on the internet. The same can be said for an officer making verbal racial slurs or posting the same as a written comment on Facebook. The need for a special policy to cover social networking is minimal if a police agency considers the actions as conduct already covered or prohibited by existing policy.

Officers should already be aware of the existing policies, and educating them with the fact that these policies cover their use of social networking would be a benefit to the officer and the agency. Once police executives recognize the social networking problems and formulate an education curriculum to deal with the issue, on duty violations can be dealt with relatively easily with existing policy. However, when dealing with the off duty usage for personal communication, agencies will have to turn to previous court decisions to effectively curtail questionable activity.

COUNTER POSITION

Undoubtedly, police officers will be quick to take the position of violation of their freedom of speech when policies are applied to questionable off duty social media activity. In fact, freedom of speech would seem to be a viable defense to off duty censorship of an officer's activity but only before a review of two leading Supreme Court cases. These cases are well-known and considered landmarks in establishing standards for public employee's speech.

In the case of Pickering v. Board of Education (1968), the Supreme Court set the standard for a public employee's freedom of speech. In this case, the court set a precedent with a two-part test. First, the speech in question must be determined as something of public concern for the employee to enjoy the protections under the first amendment. Once this determination is made, the second part of the Pickering test comes into play, which requires the government to show that the speech in question, while enjoying first amendment protection, was a detriment to the government's ability to provide services to the public. In this balancing test, the burden of proof is on the government to tip the scales in favor of discipline to the employee. Going back to the

cases of the intoxicated Washington state trooper and the Sandy Springs officer posting information about an investigation, both are examples of speech that would not fall into the category of public concern, thus avoiding the balancing test of Pickering and leading to discipline in each case.

In a second case, Garcetti v. Ceballos (2006), the Supreme Court concluded that speech made in the course of employment or as an employee of a government agency would not have protection under the first amendment. In this case, as well as with Pickering, the court is giving the government latitude to control the speech of employees in order to avoid impairment of services they provide. Both cases have far reaching implications for officers who post information detrimental to their agency, offensive in nature, or anything that lacks first amendment protection. These cases should be included in the education efforts of an agency in order to show the amount of control over speech that is given to a police agency by the Supreme Court.

Without education, officers will continue to rely on the privacy settings offered by the individual sites as a measure of control. This misplaced trust in security gives a level of comfort that ultimately results in private information becoming public. Regardless of these settings and the trust that may be placed in them, the likelihood of damaging information being released is still a concern. As in the cases of the Washington state trooper and the Sandy Springs officer, both reported their privacy settings only allowed their “friends” access to their content. The fact that the information was ultimately made public is the example of this misplaced trust officers must avoid.

CONCLUSION

Choosing Facebook as the reference for this paper was initially based on the single fact that it is at the top of the list in users and usage. Interestingly, Dwyer, Hiltz and Passerini (2007) found in their study that users of Facebook provide more private information than users of MySpace. They also determined that in contrast to MySpace, Facebook users expressed a greater amount of trust. This information is not meant to infer that Facebook is more of a concern, it just illustrates that Facebook is large, and private information is being posted by the many users. This should not diminish the concern for all social networking sites and the issues of privacy since all have their inherent risks.

Law enforcement agencies must recognize the explosive growth and potential threat in the area of social networking sites, responding with a proactive approach of education and training with emphasis on existing department policies. Research results showed that individuals, in general, are likely to ignore or rely too heavily on security settings provided by social networking sites with the benefits of usage outweighing the risks involved (Acosti & Gross, 2005; Gross & Acosti, 2006; White, 2004). The goal of police agencies should be to educate officers to the privacy issues and risks while reinforcing education and training with the application of existing policies. This could be accomplished with something as simple as a bulletin issued to all employees or a prepared in-service training session to cover the issue.

There will be detractors that see the education or training as encroaching upon the freedom of speech. The education process should include an explanation of what is covered by this freedom, or the lack thereof in many cases for government workers. If

this is dealt with from the beginning and approached as positive education that will ultimately protect the individual privacy of the officer; it may be possible to avoid the negative intrusion they may feel.

With the examples from Sandy Springs, Georgia, and Washington State, it is clear that action is needed to avoid future misconduct by officers who may not understand the implications of their use of social networking. Law enforcement agencies must respond to the lack of understanding and knowledge that the research shows exists. Education, training, and existing policies will ultimately protect the agency and the individual officer from the pitfalls that come with the use of social networking.

REFERENCES

Acquisti, A., & Gross, R. (2006). *Imagined communities: Awareness, information sharing and privacy on the Facebook.* Cambridge, UK: Robinson College.

Cranor, L., Reagle, J., & Ackerman, M. (1999). *Beyond concern: Understanding net users' attitudes about online privacy* (99.4.3). Retrieved from http://arxiv.org/html/cs/9904010/report.htm

Dwyer, C., Hiltz, S.R., & Passerini, K. (2007, August). *Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace.* Retrieved from http://www.csis.pace.edu/~dwyer/research/DwyerAMCIS2007.pdf

Facebook. (2010). *Facebook's privacy policy*. Retrieved from http://www.facebook.com/home.php?#!/policy.php?ref=pf

Fraga, B. (2010, January 5). Police investigate report of officer posting photo of dead body of Facebook. *SouthCoastTODAY.com.* Retrieved from http://www.southcoasttoday.com/apps/pbcs.dll/article?AID=/20100105/NEWS/10 50330

Garcetti v. Ceballos, 547 U.S. 410 (2006).

Gross, R., & Acquisti, A. (2005, November 7). *Information revelation and privacy in online social networks*. Paper presented at the ACM Workshop on Privacy in the Electronic Society, 2005, Alexandria, VA. Abstract retrieved from http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf

Horton, P. (2009, January 18). 2 officers lose jobs over online indiscretions. *The Tri-City Herald.* Retrieved from http://www.tri-cityherald.com/2009/01/18/449207/2-officers-lose-jobs-over-online.html

Lipford, H., Besmer, A., & Watson, J. (2008). *Understanding privacy settings in Facebook with an audience view.* In Proceedings of UPSEC '08 (Usability, Psychology, and Security). Berkeley, CA: USENIX Association.

Nielson Netview. (2010, September). *Top 10 global web parent companies, home and work.* Retrieved from http://en-us.nielsen.com/rankings/insights/rankings/internet

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

Stevens, A. (2009, December 9). Officer: Facebook postings didn't warrant firing. *The Atlanta Journal Constitution.* Retrieved from http://www.ajc.com/news/north-fulton/officer-facebook-postings-didnt-235017.html

Tenbrunsel, A.E., & Messick, D.M. (1999). Sanctioning systems, cooperation and decision construal. *Administrative Science Quarterly, 44,* 684-707.

White, T. (2004). Consumer disclosure and disclosure avoidance: A motivational framework. *Journal of Consumer Psychology, 14*(1&2), 41-51.