

# **WHAT IS YOUR NEW SOCIAL MEDIA POLICY MISSING?**

by

**Lieutenant Gwendolyn Waters  
San Bernardino Police Department**

September 2011

Command College Class 49

The Command College Futures Study Project is a FUTURES study of a particular emerging issue of relevance to law enforcement. Its purpose is NOT to predict the future; rather, to project a variety of possible scenarios useful for strategic planning in anticipation of the emerging landscape facing policing organizations.

This journal article was created using the futures forecasting process of Command College and its outcomes. Defining the future differs from analyzing the past, because it has not yet happened. In this article, methodologies have been used to discern useful alternatives to enhance the success of planners and leaders in their response to a range of possible future environments.

Managing the future means influencing it—creating, constraining and adapting to emerging trends and events in a way that optimizes the opportunities and minimizes the threats of relevance to the profession.

The views and conclusions expressed in the Command College Futures Project and journal article are those of the author, and are not necessarily those of the CA Commission on Peace Officer Standards and Training (POST).

## WHAT IS YOUR NEW SOCIAL MEDIA POLICY MISSING?

Law enforcement has always been a dangerous profession. Those who take it on willingly risk their lives to form the barrier between criminals and the rest of society. In the past, that risk was acceptable because officers could, to a large degree, protect their personal lives and loved ones from the threat they voluntarily face at work. But the scope of that threat has changed now. The power of the Internet, and especially of social media, has brought the threat home to officers and their families. The unavoidable fact is that officers now have little ability to defend their homes or their loved ones from the repercussions of a career invested in defending society from criminals.

The Internet has been widely available for public use since the early 1990's.<sup>(1)</sup> In its mere two decades of existence, it has become such an integral part of everyday life that it is already difficult to recall how society functioned without it. Compared to the brief lifespan of the Internet, social media is still in its infancy. "Social media," which began to evolve in 2003, refers to users' ability to add their own content to any website that allows it.<sup>(2)</sup> Social media sites are not static, meant only to be viewed by visitors, but can be continually modified by users who add their own commentary, photos, video, etc. Facebook and Wikipedia are two well-known examples.

With the advent of social media, the Internet is no longer a fixed object to be passively observed but has become a dynamic venue for proactive, and often passionate, involvement. The growth of social media, and its corresponding power and influence, has been phenomenal.<sup>(3)</sup> In just a few years, it has created shockwaves that reverberate throughout society. Both the decline of traditional newspapers<sup>(4)(5)</sup> and the outcome of the 2008 presidential election<sup>(6)(7)</sup> have been

attributed to it. Law enforcement agencies have not neglected to notice the influence of social media. Many departments have adopted or are drafting policies or regulations addressing how their employees use this new networking engine. But the vast majority of these policies are missing a crucial aspect of the issue. While agencies are concerned with protecting themselves from liability by controlling what officers post online, they neglect the fact that they have an important responsibility to their officers as well.

“Public” information, available from such sources as birth, death and real estate records, has been available online for years. Social media has raised the threat level of this data being readily available by greatly increasing the amount and type of personal information exposed while drawing a much larger audience online to find and use it. Social media is an entirely new beast with a unique nature that makes it singularly powerful and unpredictable. Characteristics of social media that combine to make it especially threatening to law enforcement include:

- Narcissism – The very structure of social media encourages self-promotion.<sup>(8)</sup> It offers easy access to an unlimited pool of potential “friends,” allowing individuals who crave validation to achieve a feeling of connection or popularity not available in their offline lives. Therefore, it attracts a high percentage of individuals who are driven by a desire for attention, notoriety, or “fame.” To gain that attention, the goal is to post information that is entertaining or provocative.
- Anonymity – The seemingly anonymous environment online also encourages users toward inflammatory and shocking behavior. Individuals can create screen names or entirely new identities that allow them to act outside their normal inhibitions or self-restraint. This anonymity emboldens people to say or do things they otherwise wouldn’t while also hampering any effort to control such activity.<sup>(9)(10)</sup>

- Lack of “media” restraint – Constraints that keep traditional media in check do not exist for social media. Law enforcement has always had a tenuous relationship at best with the traditional media. Good news about officers’ hard work and integrity does not sell papers; exposés about corruption and abuse of authority do. What has always kept the relationship in balance is that traditional media must maintain some level of ethical standards. The media source’s credibility and, therefore, its marketability are at stake. With social media, no such restraints exist. Anyone can post anything online with little fear of repercussion and this emboldens people toward more inflammatory, and less ethical, activity.
- Online crowd mentality / copycat behavior – A natural pooling of like minds occurs online. This bolsters confidence and the impression of support for what may otherwise be socially unacceptable behavior. Copycat behavior may make the first well-publicized transgression the impetus for many more. Social media also engenders a mob mentality wherein one small stimulus can spur a wide-scale reaction that feeds on itself to grow out of control.<sup>(11)</sup> Incidents generated or accelerated through social media have the ability to develop faster and spread farther more rapidly than anything society has dealt with before.
- “Cooling off” period eliminated – In the past, simple protections like a post office box and confidentiality on license plates provided a level of protection for officers that is ineffective today. Instant access to private information eliminates the time and effort it took in the past for an individual to learn personal facts about an officer. That instantaneous access also, therefore, eliminates any cooling off period during which an individual might reconsider acting on the anger or resentment often engendered by

contacts with police. An outraged individual could easily be on an officer's doorstep before the end of his shift, when the officer is not present to defend his home or his family. That was the case in Gooding, Idaho in 2009 when, shortly after the service of a search warrant, several rounds were fired into an involved officer's home while his wife and son slept inside.<sup>(12)</sup> Gooding is a very small town where members of the police department are known personally by much of the community so no Internet search was necessary for the assailants to learn where the officer lived. But social media has, in effect, made the entire world a small town where an unlimited community of people has access to information that once was considered personal.

These factors coalesce to make social media a uniquely significant social force that constantly seeks a point of focus. Characteristics intrinsic to law enforcement make it a natural focal point for that energy:

- Law enforcement is a public profession - Law enforcement activities necessarily occur in a public arena and officers have very little right to their own privacy in the performance of their duties. Social media has exponentially increased that exposure. Officers are now constantly surrounded by cameras and amateur "reporters" with the ability to broadcast every police action, and their opinion of it, to a worldwide audience. Because of its public nature, law enforcement provides an easy topic for social media discussion.
- Law enforcement is inherently fascinating and controversial – Police work involves drama, intrigue, excitement and the eternal battle between good and evil. Society is captivated by it, as is demonstrated by the number of crime dramas on television and in theaters. Added to this is the fact that the police officer's role is often ambiguous. While

expected to be on the side of good, officers are human and therefore fallible. They are also often resented by the public they are entrusted to protect simply by people who don't appreciate enforcement of the law when they are on the wrong side of it. So peace officers are extremely controversial figures, with society both needing and wanting their services and at the same time often resenting them and craving their downfall.

- Conflict is intrinsic to the profession – Law enforcement necessarily pits officers against the most lawless element of society. With increased exposure of personal information through social media, reliance is now entirely on socially or morally based self-restraint, or intimidation through criminal sanctions, to prevent antagonists from crossing the invisible line that separates an officer's professional and personal lives. But, as a main function of the job is to confront those who are actively demonstrating a lack of respect for the law or the rights and welfare of others, neither self-restraint nor respect for the law can be considered a strength of the target population.

The nature of social media and of law enforcement make the relationship between the two particularly volatile. While few significant issues have yet arisen, the potential exists for social media to impact law enforcement in a number of ways, such as by attacks on officer credibility or through cop-baiting.

Personal credibility is essential to peace officers. Once an officer's integrity is compromised, he becomes worthless for courtroom testimony and a liability to any investigation. Through social media, people have the power to attack an officer's credibility which, even if utterly erroneous, can reach a significant audience. The next time there is a major police "scandal," more people than ever will follow it online and the potential exists for denigration of

officers to become a popular pastime. Not only can the involved officers' credibility be permanently damaged and the outcome of the case swayed, but any officer at any time could find his integrity under serious attack online, with that information available to potential jurors or Internal Affairs investigators. There have already been several cases where comments posted by officers on social media sites have led to discipline or impeachment. Such behavior has been a key focus of the social media policies already put in place. More insidious, though, are postings by members of the public, over which departments have no control. Negative comments, once viewed, may create an immutable impression in the mind of the viewer regardless of their veracity.

Cop-baiting could present an even more critical crisis for law enforcement. Video of officers behaving badly makes great YouTube fare. It can also be financially rewarding since a claim or lawsuit could follow. A citation or jail time would be worth it to a lot of people if a cash payoff might result. Empowered by social media, cop-baiting may become common enough that officers will never know if the situation they're facing is legitimate or one that is being staged or at least exaggerated for fame or profit. Cop-baiting can also create a financial crisis for departments if litigation from numerous incidents results.

Many police professionals will recall the 1989 incident involving the Long Beach Police Department in California. To expose what he perceived as mistreatment of minorities, Don Jackson, a former sergeant with the Hawthorne Police Department, had an NBC-TV camera crew follow him and secretly videotape as he was stopped by Long Beach officers for an alleged traffic violation. During his detention, the video captures one of the officers apparently shoving Jackson into a plate glass window, shattering the glass. While misdemeanor charges against both officers were dismissed, their careers both ended in stress retirements and the Department paid a

\$170,000 settlement to avoid the higher cost of a civil trial.<sup>(13)</sup> Jackson's credibility as a former police sergeant undoubtedly helped him gain the support of a major news network in documenting his "sting." With the new power and scope of social media, no legitimate media backing is necessary. Whether the goal is a political statement, social activism, fame or financial gain, everyone now has the ability to conduct their own "sting operation" and broadcast it to the world.

While possibilities like these have the potential to create considerable problems, the greatest danger lies in the personal threat to officers and their families. Due to social media, officers are now public figures to a much greater degree than ever before, and at the same time barriers between their professional and personal lives have been virtually eliminated. They can have no expectation now that the danger they face on the job won't be brought to their homes and their families. Complicating the issue further, motivated individuals could destroy an officer's sense of security without breaking a single law. With just an officer's name and Internet access on a cell phone, an antagonistic traffic violator could have a satellite image of an officer's home displayed on his phone when the officer approaches to issue the cite. A seemingly innocuous note could be left on an officer's front door; a photo of a child could be posted on a social networking site with an ostensibly innocent comment such as, "Isn't Officer So-and-so's daughter cute?"

A glimpse into the future for all law enforcement agencies may have been provided recently by the repeated hacking of the computer systems of Arizona's Department of Public Safety. As a statement against Senate Bill 1070, Arizona's immigration law, anonymous individuals hacked into the agency's computer servers and publically posted information obtained from them, including home addresses of officers and the identities of undercover

operatives.<sup>(14)</sup> A group calling itself “AntiSec,” for Anti Security Movement, took credit for the acts, stating that one of their specific goals was to jeopardize the officers’ safety: “Yes we’re aware that putting the pigs on blast...risks their safety....We are making sure they experience just a taste of the same kind of violence and terror they dish out.”<sup>(15)</sup> These well-publicized and very personal attacks on officers may very well serve to incubate similar ideas in the minds of others.

Unfortunately, this is a situation where it is much easier to identify the problem than the solution. The Internet is not under local, state or even federal control. It is an international entity that exists well beyond most judicial or governmental jurisdiction. A myriad of laws provide various protections, but none are comprehensive or effective enough to prevent the kinds of issues that could be devastating for officers and for the law enforcement industry. The growth of social media has simply outpaced any attempts to legislate control of it. Until effective legal protections are devised, internal management mechanisms can and should be implemented to limit the exposure of police employees to this job-related threat.

To provide the most effective protection possible, an employee or unit within a each law enforcement agency should be tasked with Social Media Management responsibilities. Their core functions should include:

- Providing ongoing training for personnel on current issues and self-protection. Educating employees on the hazards of social media and what they can do to protect themselves is essential to minimizing the threat. One-time training is not sufficient in the face of social media’s rapidly changing terrain. Employees cannot be expected to have the time or expertise to keep up with its constant evolution. A dedicated social media manager

should keep personnel updated through e-mails, memoranda, briefing trainings, etc, regarding new hazards and improved defenses

- Following procedures to remove employees' personal information from sites that post it. There are numerous sites that provide personal information such as home addresses from public records. Most will remove that information if petitioned to do so, but each has its own procedures for making that request. These sites also need to be monitored in case the information reappears. Expecting each employee to locate every site and determine how to have their information removed would be inefficient. A social media manager could facilitate the process and ensure consistency for all personnel
- Establishing Internet and social media alerts on employees and the agency. Several sites or search engines offer services, many free of charge, that provide e-mail notification any time a name or term is mentioned or searched online. Google Alerts, TweetBeep, SocialMention, and BoardTracker are a few examples. Alerts on personnel could be directed to their private e-mail to avoid conflict with employee unions over privacy of off-duty activities. Alerts on the agency should be monitored by the social media manager
- Monitoring, or listening to, social media activities in relation to the department and its personnel. Many businesses have realized that "listening" in on social media conversations can provide a wealth of information on consumer trends, along with the strengths and weaknesses of a particular item or brand. Law enforcement agencies could similarly benefit from listening for commentary about the department, its programs, and its personnel. This would allow the department not only to capitalize on its strengths, but to identify and mitigate developing negative images or potential threats. Providing the

most effective protection against an impending attack requires identifying the threat early and strategizing a defense. Consistent monitoring of social media would provide an early warning system against any threats developing or discussed online.

- Monitoring industry-wide activity for trends or incidents that might precipitate copycat behavior. Beyond online listening about one's own department, attention must be paid to incidents occurring industry-wide, because one episode could quickly precipitate others. Empowered by social media, issues can develop more rapidly and spread more widely than anything law enforcement has dealt with in the past. In the AntiSec hacking of Arizona DPS, the FBI has arrested several of the individuals involved. AntiSec then turned their offensive against the FBI, hacking into its server and obtaining information on more than 7,000 officers. They then demanded charges against the AntiSec defendants be dropped and called on others to join their cause: "To our hacker comrades: now is the time to unite and fight back against our common oppressors. Escalate attacks against government, corporate, law enforcement and military targets: destroy their systems and leak their private data." They also issued a challenge to law enforcement: "Arrest us. We dare you."<sup>(16)</sup> This case might ultimately involve only a small number of individuals with fringe anti-government beliefs and advanced computer skills. Strengthened by social media, though, they have already caused widespread damage and instilled the idea in others. The best defense against such a threat is to recognize it as early as possible and identify ways in which an agency's defenses might be bolstered against it.
- Maximizing use of existing laws / Advocating for more effective laws. Laws concerning social media are evolving as quickly as social media itself. Expertise needs to be applied

to knowing the legal protections that are available before an incident occurs and taking advantage of any opportunity to support the development of laws that will provide real defenses.

Protecting employees from the kind of threats so easily propagated through social media will not only benefit the employees but is in the best interest of agencies as well. Significant costs can result from compromised officer credibility, damaged department image, relocation costs associated with credible personal threats, etc. It is time for the law enforcement industry to acknowledge the heightened level of threat the social media presents. Hoping that large-scale impacts won't occur will not lessen the costs to law enforcement when they do; proactively addressing the threat will.

Until some kind of effective legal protections are developed, the best defense is awareness, education, and diligent management of employees' online exposure. While these actions won't entirely protect officers and agencies from the kind of hazards social media presents, they will minimize exposure and provide the greatest level of defense currently available.

## Conclusion

It is often more cost effective to wait and see what problems arise before developing solutions than to take preventive actions that might not be necessary. The problem with that approach in this situation is that if the relationship between law enforcement and social media blows up, it has the potential to blow in a very big way, to the detriment of officers, agencies, and the industry. Social media has an extraordinary ability to generate momentum, and law

enforcement provides a natural stimulus and accelerator for that momentum. They can easily combine to create a perfect storm that could be devastating for officers and for the industry. The question is whether police agencies will incorporate into their social media policies their responsibility for protecting employees from this profoundly increased level of job-related threat before they are blindsided by a sudden “viral” attack on officers.

---

Endnotes

<sup>1</sup> Vinton G. Cerf and others, “A Brief History of the Internet,” the Internet Society (December 2003). <http://www.isoc.org/internet/history/brief.shtml>.

<sup>2</sup> Andreas M. Kaplan and Michael Haenlein, “Users of the World, Unite! The Challenges and Opportunities of Social Media.” *Business Horizons*, Volume 53 Issue 1 (2010): 59-68.

<sup>3</sup> Ibid.

<sup>4</sup> State of the News Media 2010 Executive Summary. The Pew Research Center’s Project for Excellence in Journalism; [http://www.stateofthemedial.org/2010/chapter%20pdfs/2010\\_execsummary.pdf](http://www.stateofthemedial.org/2010/chapter%20pdfs/2010_execsummary.pdf).

<sup>5</sup> Jon Katz, “Online or Not, Newspapers Suck,” *Wired Magazine*, Issue 2.09 (2009). <http://www.wired.com/wired/archive/2.09.news.suck.html>.

<sup>6</sup> Erik Qualman, *Socialnomics: How Social Media Transforms the Way We Live and Do Business*, (New Jersey: John Wiley & Sons, 2009).

<sup>7</sup> Michael Cornfield, “Yes, It Did Make a Difference,” 2008; <http://takingnote.tcf.org/2008/06/yes-it-did-make.html>.

<sup>8</sup> Christine Rosen, “Virtual Friendship and the New Narcissism,” *The New Atlantis* (Summer 2007): 15-31.

<sup>9</sup> Deborah G. Johnson, “Ethics Online,” *Communications of the ACM*, Vol. 40 No. 1 (January 1997): 60-65.

<sup>10</sup> Julie Zhuo, “Where Anonymity Breeds Contempt,” *The New York Times*, November 29, 2010; <http://www.nytimes.com/2010/11/30/opinion/30zhuo.html>.

<sup>11</sup> Russ, Christian, “Online Crowds – Extraordinary Mass Behavior on the Internet,” 2007. [http://i-know.tugraz.at/wp-content/uploads/2008/11/8\\_online-crowds.pdf](http://i-know.tugraz.at/wp-content/uploads/2008/11/8_online-crowds.pdf).

<sup>12</sup> Alyson Outen, “Officer’s Home Sprayed with Bullets, No One Injured,” KTVB.com. <http://www.ktvb.com/news/Officers-home-sprayed-with-bullets-no-one-injured-79832692.html#>.

<sup>13</sup> Edward J. Boyer, “Alleged Police Abuse Case is Settled,” *Los Angeles Times*, October 12, 1994. [http://articles.latimes.com/print/1994-10-12/local/me-49365\\_1\\_long-beach](http://articles.latimes.com/print/1994-10-12/local/me-49365_1_long-beach).

<sup>14</sup> Marc Lacey and Richard A. Oppel Jr, “Hacked Memos of State Police in Arizona are Released,” *New York Times*, June 24, 2011. [www.nytimes.com/2011/06/25/us/25hack.html](http://www.nytimes.com/2011/06/25/us/25hack.html).

<sup>15</sup> “AntiSec ‘Hackers Without Borders’ Claim New Hack on Arizona State Police,” *Los Angeles Times*, June 29, 2011. <http://latimesblogs.latimes.com/technology/2011/06/antisec-hackers-lead-files-said-to-be-from-arizona-state-police.html>.

<sup>16</sup> Steve Raga, “AntiSec: 77 Law Enforcement Websites Hit in Mass Attack,” *the Tech Herald*, July 31, 2011. <http://www.thetechherald.com/article/php/201130/7447/AntiSec-77-law-enforcement-websites-hit-in-mass-attack>.