Social Media Sample Policy Supplemental Resource Considerations

9-8-21

The materials provided in this correspondence are for general informational and educational purposes only and are not intended to be and should not be considered legal advice or opinions. Prior to making any policy or rule changes seek the advice of your municipal attorney.

J.A. Montgomery CONSULTING

Intelligence Alert

Off-Duty Social Networking Warning

December 10, 2009

Summary. The South Florida HIDTA Intelligence Center has been advised of a new legal maneuver used by defense attorneys who are on the prowl to discredit the character and integrity of the prosecution's witnesses.

Background:

There is a new proverb being issued to the law enforcement community at large – beware of what you post on social networking sites – everything can be held against you in a court of law. It is a growing trend among defense attorneys to perform Google and Yahoo name searches to check out witnesses before going to trial. Earlier this year in a New York State Court, what should have been a "slam-dunk ex-con with a gun case," resulted in an acquittal for the defendant. The defendant, who was on parole for a burglary conviction when he was arrested, beat the most serious charge—a felony possession of a 9 mm Beretta and a bagful of ammunition. Instead, the NYPD officer was impeached for posting material on his personal social networking sites just prior to the arrest, which perceived him as a rouge cop.

Warning

Warning to law enforcement officers who display objectionable content on social networking sites – what you post can be held against you.

Prior to the trial, the jury had learned that besides setting his mood indicator to "devious" on his MySpace page , he had announced on his Facebook page that he was watching the movie, "Training Day" (a film depicting corrupt police behavior and brutality) in order to brush up on proper police procedures. The "Devious" setting is one of 122 mood indicators and comes with an angry, red emoticon of a facial expression, which is being licked by flames.

Attorneys also introduced the officer's self-incriminating remarks about Internet video clips of police arrests to the jury: "If he wanted to tune him up some, he should have delayed cuffing him," and, "If you were going to hit a cuffed suspect, at least get your money's worth 'cause now he's going to get disciplined for a relatively light punch."

Since convictions rest on the credibility of the officer, the defense strategy illustrated to the jury that what the officer had written on social network websites is how he "really" conducts police work, thereby holding the officer to the words he had written in cyber space.

The suspect in this case had claimed that the officer had used excessive force on him, leaving him with three broken ribs. The suspect also alleged that when the police officer realized that he had to explain the broken ribs, he "planted" a stolen 9mm Beretta and charged him with it. The officer claimed that his Internet

Intelligence Alert

Off-Duty Social Networking Warning

December 10, 2009

persona was simply bravado, similar to what might be said in a locker room; the only difference is that one of them is preserved on a digital server.

Another illustration of poor judgment comes from an Indiana officer who described his job on his personal Facebook as a "garbage man" who picks up "trash" for a living . He also posted photographs of himself pointing a gun at another officer's head while holding a beer off-duty. Both officers had been drinking alcohol, which one officer personally validated when he posted that they were "drinking lots of beer" that day. Another comment read, "These people should have died when they were young anyway, I'm just doing them a favor."

The law enforcement community is urged to exercise caution and contemplate the tactical significance of their comments, jokes and photographs before releasing them into cyberspace where they will be preserved on a digital server available for subpoena for all eternity. This includes the contents of writings, recordings or photographs on sites such as Facebook, MySpace, Twitter, YouTube, Internet chat rooms, e-mail, text messages, answering machine greetings, and voice mail messages.

Sources.

Los Angeles County Sheriff's Department. *Impeachment via Social Networking Websites*. Newsletter, May 27, 2009

Dwyer, Jim. *The Officer Who Posted Too Much on MySpace. New York Times,* 10 March 2009. http://www.nytimes.com/2009/02/11/nyregion/11about.html

Timothy D. Wagner
Director
SFLHIDTA

Joel Widell
Deputy Director
SFLHIDTA

Gary F. Grimm
Coordinator
SFLHIDTA Intelligence Center

Tel: 954-.430.4700

Fax: 954.430.4708

LOS ANGELES COUNTY SHERIFF'S DEPARTMENT
COURT SERVICES DIVISION

Information Bulletin

REAL TIME, RIGHT NOW, RIGHT CHOICE

February 2010

CHP GETS SUED FOR LEAKING PHOTOS

On October 31, 2006, Nicole Catsouras died at the age of 18 years old after she lost control of her father's Porsche 911 Cabrera.

California Highway Patrol officers took some gruesome photographs of Ms. Catsouras, as part of the traffic accident investigation.

Unfortunately, some of these photos were sent to others within the Department and the photos were eventually posted on the Internet.

One CHP employee was heavily disciplined and a second employee resigned behind leaking the photographs.

The Catsouras family sued the CHP. In March 2008, the judge dismissed the case filed by the Catsouras family.

On February 1, 2010, the California Courts of Appeal overturned the ruling by the judge and the family can continue with the lawsuit against the CHP.

INTERNET PHOTOS OF JUROR/CELEBRITY

On February 1, 2010, a young actress was serving jury duty at a Los Angeles area courthouse. The actress was serving without the knowledge of the media.

A Court Services Division employee was photographed in uniform with the actress at the courthouse. The employee sent the photo to several friends. The photo was forwarded to others. Eventually the photo containing the uniformed member and the actress was placed on Facebook.

Somehow the media learned the photo was posted on the Internet, resulting in the paparazzi staging in front of her residence. The actress' attorney commented that the actress was now in fear for her safety.

REAL TIME, RIGHT NOW, RIGHT CHOICE

The two incidents cited have huge differences, but the bottom line is that the choices made by an individual can have a HUGE impact on one's personal life, career, liability, and can tarnish the reputation of the Department and its members.

Today, **Right Now,** we live in a world of **"Real Time"** where the choices we make and the actions we take can be placed online for the entire world to see.

Every day each one of us must **MAKE THE RIGHT CHOICE and TAKE THE APPROPRIATE ACTION!**

POLICE
THE LAW ENFORCEMENT MAGAZINE
COMMUNITY FOR COPS

Cover Story

December 2009

Watch What You Post

Social networking sites are great for meeting new people and having some fun, but don't let that fun kill your career.

by Dean Scoville

Cops, like any other members of a high-stress profession, like to joke around about what happens at work. Many of these jokes would be considered crude or insensitive, perhaps even slanderous, by people who don't work as police officers. But as long as the public doesn't hear these jokes then the attitude of most administrators is no harm, no foul.

Unfortunately, such cop jokes are now being voiced in public. A generation ago, when cops wanted to blow off steam, they met some place private, had a few beers, and nobody outside the circle knew what was said or done.

Today's cops may still gather over a case of cold beer, but they also gather online using social networking tools such as MySpace and Facebook. Which is a problem for agencies and officers because what many users of social networks don't realize before its too late is that anything they do or say or write on these sites is done so in full view of the public. Other officers may be aware that they are speaking in public, but they apparently don't care.

The Cromer Case

Perhaps the most widely known example of an officer coming to grief because of something that he or she wrote on a social networking site happened three years ago in Kentucky.

In 2006 Officer Joshua Cromer of the Lexington Police Department made a traffic stop. The driver was country singing star John Michael Montgomery who lives nearby. Cromer arrested Montgomery and the singer was later charged with driving under the influence, possessing a controlled drug, and two counts of carrying a concealed deadly weapon. Montgomery later pleaded out on the drunken-driving charge. That should have been the end of the matter.

Unfortunately for Cromer, that traffic stop was just the beginning of a long nightmare. The arrest became fodder for Cromer's MySpace page. Friends, mostly fellow cops, congratulated him on the bust and poked fun at Montgomery by posting a doctored photo that showed Cromer as an adoring fan.

Complaints about Cromer's site led to the brass checking out a number of their officers' MySpace pages. What they found made them really angry. There were comments about the department, comments about the people of Lexington, comments about gays, and comments about the mentally disabled. And a very brown and very smelly storm gathered over the heads of Cromer and several other Lexington PD officers.

Cromer was dismissed from the Lexington PD on grounds of misconduct, inefficiency, insubordination, and conduct unbecoming a police officer. He later sued for back pay and reinstatement. He lost. As for the other members of Cromer's MySpace circle of friends, five of them were suspended. They were later allowed to return to duty.

Chief Concerns

The Cromer case is a clear example of an employer's ability to monitor an employee's online social network activity even away from the job. It also illustrates the power that an agency has over its officers' ability to exercise free speech.

For law enforcement officers, other public officials, and even private employees, caution should be the byword when posting material on a social networking site. And make no mistake, many agencies are monitoring what their officers do online.

These agencies know there is a potential for an employee's Website comment to become instrumental in a civil or even criminal case. Defense attorneys and civil rights attorneys are monitoring what you write on your private pages the same way that police investigators monitor the sites of criminals. So use your brain. If you don't want your comments read in public, don't post them in public.

And whatever you do, don't maintain your Facebook page on the job. An Indiana State Trooper found himself under investigation for his online activity both off and on the job.

A born multitasker, this trooper allegedly bragged about his heavy drinking, posted a picture of his cruiser with collision damage and the caption "Oops! Where did my front end go?" and uploaded an image of a gun being pointed at his head. On the same Facebook page, he reportedly characterized himself as a "garbage man," saying, "I pick up trash for a living." Statements reflecting dissatisfaction with weather and working conditions were also allegedly posted during times that the trooper was supposed to be at work.

When a TV news report revealed the evidence to state patrol brass, they launched an internal investigation. At presstime, the findings of that inquiry have not been released.

With Friends Like These

The nature of social networking sites, which link users to hundreds-even thousands-of online friends, can also make them particularly hazardous for your career. Just ask Officer John Nohejl of the New Port Richey (Fla.) Police Department.

By all accounts, Nohejl accomplished great things during his three years as a school resource officer, turning a D school around into an A school in one year. Well liked by the kids and school staff, Nohejl

came up with the idea of setting up a MySpace page to communicate with students. School leaders, parents, and the police department were enthusiastic about the idea. In a relatively short period of time, Nohejl was not only able to share safety tips with students via the new "Officer John" site but also obtain tips that expedited investigations and resulted in arrests.

But then he found himself in a peck of trouble.

An anonymous complainant advised the department that one of Nohejl's MySpace "friends" offered a link that included photos of nude women. Another offered obscene comments about oral sex and large breasts, among other objectionable content-all of which could be easily navigated to by 11- to 14-year-old students visiting Nohejl's page.

Now the links are gone, but the sting of the experience still lingers for Nohejl.

"I tried to do a good thing for kids," Nohejl reflects. "But I got blind-sided. I'd checked out this person's profile and it seemed OK, so I allowed him on as a friend. But once I did that, he went back onto MySpace and maliciously changed his profile so that in a matter of three clicks from my page, kids could be exposed to this pornography. I was railroaded-not by the department, but by the person who orchestrated this mess."

The Florida attorney general's cybercrime task force investigated the Nohejl case. Nohejl was cleared of any wrong-doing. Unfortunately, a collateral casualty was the Officer John MySpace account. "The moment this problem was brought to light, they immediately removed it," Nohejl says.

Back on patrol these days, Nohejl hopes that others learn from his experience. "It's a good lesson for cops. You can be held responsible for things that are beyond your control," Nohejl says. "Who can possibly go through the profiles of hundreds of MySpace friends every day to make sure that someone's not going to do the same thing again?"

Etiquette and Policy

Concerns about such sites go beyond objectionable material or technological access by hackers. By piecing together information about companies through their employees' social network entries, identity thieves and others have been able to trick people into allowing confidential information beyond intended audiences.

Consequently, many agencies feel under pressure to establish some form of social networking etiquette or protocol for their employees. As a result, some agencies are just telling their employees to stay off Facebook and similar sites.

Former police officer, academy instructor, and network security author Deb Shinder suspects that until some new legal precedent dictates otherwise, agencies may have the upper hand in this equation.

"Unless there is state law or a union contract that says otherwise, [police departments] can be pretty much as stringent as they want to, as long as the policies are applied equally and without discrimination," Shinder says.

But can your employer really tell you what you can and can't do with your own computer on your own time?

Maybe. "Off-duty activities on one's own computer are more of an issue of contention," explains Shinder. "But even if the agency doesn't have a policy specifically addressing online behavior, certain online activities–especially if the person's profile and social networking posts are open to the public–could probably be construed to fall under general 'conduct unbecoming' regulations."

Nonetheless, Shinder believes that agencies would be ill advised to prohibit their officers from enjoying the benefits of social networking online. "Young people who grow up with social networking as part of their lives aren't going to take well to being told they can't do it anymore, and law enforcement will lose way too many potential good cops if they take a hard line on that," she explains.

Given that social networking is here to stay and young cops believe they have a fundamental right to use these sites, smart agencies are going to have to find a way to regulate what officers do online without being too restrictive.

"I think it makes more sense to cautiously embrace the technology, to set policies that are reasonable, and to educate officers about what does and doesn't constitute professional online behavior and more importantly, why their online behavior matters, why it's in their own best interest, not just that of the agency, for them to project a public image that they won't cringe over a few years down the line when they're trying to move up the career ladder," says Shinder.

Some agencies are adding online social network regulations to their policy manuals.

For example, the Indiana State Police is in the process of drafting standard operating procedure for its staff regarding posting information on personal Web pages such as Facebook. And in Salt Lake City, Sgt. Robin Snyder, a public relations officer with the city police, is currently researching laws and other department policies toward formulating a policy for her department.

Others have already set their policies. The Minneapolis Police Department adopted a policy in October that prohibits its police officers from identifying themselves as such on social networking sites.

Officer Reaction

The implementation of such policies has taken some cops aback.

"Cops are not only being held to higher standards," notes one Massachusetts police officer, "but in some cases, unreasonable standards."

Many officers say the "do as I say, not as I do" posture of some agencies is especially annoying, as their employers and commanders see themselves uniquely capable of maintaining professional online content. Others say they don't appreciate the interference in their personal lives.

"It's like freedom of speech, apparently there are some who think you should be able to tell a cop to go expletive himself without repercussion and yet they also believe that a cop should be disciplined for using any profanity (called command presence when I write my report or testify in court). Shouldn't then a social network profile be freedom of speech?" asked one officer.

And while many officers understand the impetus for anti-social networking policies, they still resent them.

"It's all about liability. We have enough of that stuff already as cops, I'm not giving anyone another weapon to try and take my job away."

Use Common Sense Online

Salt Lake City PD's Snyder can only shake her head when she contemplates some of the trouble cops have gotten themselves in behind social networks.

"It seems that police officers have more common sense when it comes to using their gun in the field if they have to," Snyder notes. "When they go into a restaurant, they know to sit with their back to the wall, they know if something happens where their escape routes are. But they never think about if they post something on Facebook. Are they going to offend somebody racially or by sexual orientation? They never think about that kind of stuff. Officers should know better than to post certain things on Facebook."

To this end, Snyder tries to pick up the slack.

"I teach a media relations class to the recruits," Snyder says. "I've added social media to tell them that they're no longer anonymous. I ask how many people have Facebook accounts, and I tell them they have to think about if they post something and their local news media picks it up. There's no official social networking training, but I see it coming within the next year."

Shinder offers the following pointers when engaging in social networking: "Don't post pictures of yourself doing something embarrassing or illegal. Don't make derogatory comments about any race or group. Don't post comments that could be construed as sexually harassing, especially if you have co-workers or subordinates of the opposite gender as 'friends.' It's also probably a good idea not to get into passionate diatribes about agency politics."

It is also important to point out that your friends not only see what you post on your site, but also what your other friends post there. "That's another reason to separate your professional and personal lives by having more than one Facebook or MySpace account," asserts Shinder.

Most sites do let you set options regarding which of your friends can see what types of posts, and it's a good idea to become very well acquainted with how these tools work and use them.

Sam Walker, a retired professor and a former member of the National Board of the American Civil Liberties Union, suggests that a simple disclaimer by the employee may protect many officers from earning the ire of their departments.

In the absence of policies developed to specifically address social networks, many agencies have and will probably continue to flag their personnel under some generic catch-all: Conduct unbecoming a peace officer. But they will address it.

Curiously, none will come near to invoking the caveat most invoked in matters of law enforcement concern: Use common sense.

For in matters of social intercourse, there is little commonly agreed upon and what may be acceptable to one person or group may well be unacceptable–even offensive–to another.

In the meantime, it would appear that some agencies are hoping that by adopting more rigid postures, they might wear their employees down so that they'll take a note from the Gershwin song when it comes to posting to social networks and just call the whole thing off.

PoliceOne.com News

08/06/2010

Social Media & Law Enforcement
with Lauri Stevens

Update on social media policies for law enforcement

The following article originally appeared on ConnectedCOPS.

Social media policy in law enforcement is a hot topic and well it should be. No one can or should dispute that the importance of sound policy, and the need to guide law officers in proper behavior and procedure online, is huge. Just when you're getting a handle on the elements of a good social media communication policy, and you're thinking your social media investigations need to be covered by policy as well... If you're vetting potential new officers on the Internet, you'll need a third policy for cyber-vetting of new recruits too. I'm no HR professional, but the legal ramifications in this area could be gigantic. This is an overview of some important considerations for all three social media policies.

Related Article:

The C.O.P.P.S. social media method for officers

Slightly less than a year ago, I wrote for the first time on social media policy in law enforcement. Much of what should be in a law enforcement social media policy (copyright, fair use, truthfulness, and the like as covered in the original article) is in every good social media policy. I especially like the policies of the Air Force, IBM, and Intel. But while that's true, there are several areas that are unique to law enforcement. These were also covered in my original article. Here, I offer here a couple of new insights.

I. Communication Policy / General Use

I have added two items (numbers eight and nine) to the list of areas unique to law enforcement since writing the original article, but haven't changed the rest.

1. Integrity. Perhaps the most important part of everything a law enforcement agency does online or elsewhere is integrity. Agency participants in social media should be reminded that integrity is the essential ingredient to using social media ethically. Agency employees should, therefore, be honest in their use of social media and maintain high regard for the public interest. All information disseminated should be absolutely accurate.

2. Disclaimers. Because you may be giving your personnel the authority to comment on issues relating to the department, it's imperative to emphasize the importance that officers, especially, state that what they write is their own opinion and not that of the department.

3. Identity. Some bloggers work anonymously, using pseudonyms or false screen names. Law enforcement agencies should absolutely insist that in blogs, wikis or other forms of online participation that relate to the department or the city, or activities or issues with which the department is engaged; department employees use their accurate identity.

4. Department-sanctioned tools. While it should be stated that the social media policy of the agency

covers activity by agency employees on tools they may create on their own or those of others that they might contribute to, department-sanctioned tools should be governed more closely. Careful distinction needs to be made between on and off duty work online.

5. Competence. Department employees, whether staff or sworn, should not use any social media tool unless they really understand how it works. Many of the problems with officers getting themselves into trouble happen on Facebook and often the officer(s) involved indicate they didn't know Facebook worked the way it does. Make your staff responsible for assuring their competence online.

6. Command Staff responsibility. Standard disclaimers, do not by themselves, exempt command staff officers from any special responsibility. By virtue of their position, they must consider whether personal thoughts they publish may be misunderstood as expressing opinions of the agency.

7. Training. Provide social media training for your officers and staff. Once your policy is written, be sure to distribute it with conversations about departmental support for social media.

8. What's not OK to post. This may include things such as department identification (patches, insignia, officers in uniform) and sensitive information or any other information that could reflect negatively on the department.

9. Implications on career. All violations of policy or misbehavior online could have detrimental effects on an officer's career. But one that doesn't seem obvious to all is the effect simply having a social media profile, even if there's never a problem, could have on an officer's future ability to perform undercover work. Tremendous care is warranted so than an UC officer can't be identified online.

II. Cyber-Vetting Policy

1. Notice and Consent

• ***Informing applicants.*** It's absolutely essential to let applicants know that you'll be conducting a search of their social networking profiles. Your policy should state that they will be told and at what point in the process they will be told. Some agencies don't want to give them a lot of notice so the profiles don't get altered, but surprising them altogether may not be fair.

• ***Consequences of not giving consent.*** Consent needs to be given to search a person's online profiles, especially if the agency expects to search password-protected sites. The applicant should be told that not giving his or her consent could disqualify him or her from consideration.

• ***Type of information investigator may collect.*** Will it be ok for your agency to speak with the online friends of your applicants? Some people are really taken aback by this but is it different from visiting their neighbors? Define circumstances under which agency may contact online friends and otherwise define of the scope of the search, inform the candidate, and consistently apply it to all applicants.

2. Quality Assurance & Training

• ***Internet search training for investigators.*** The world of online media is complex. Investigators need to understand the nuances of privacy settings, imposter pages, gathering and storing of evidence.

• ***How they're monitored.*** What procedures are in place to make sure the investigator is operating professionally and securely?

• ***Ongoing refresher training.*** Because platforms like Facebook changes the rules regularly and because there are always new platforms of which you need to be aware, make sure the investigator attends training at regular intervals.

3. Internet Search Practices

• ***Who can conduct searches?*** The answer is definitely, positively NOT – "the intern". That seems obvious to most but it's happened. The procedure for determining personnel authorized to perform such searches needs to be defined as well as the ongoing method by which one will be qualified to remain authorized. Should this position be defined as sensitive and receive all the protections therein?

• ***Outline expectation for notification of changes.*** Do you want to go so far as to require employees to notify you of any changes to their online profiles, such as new profiles they might have?

• ***Disclosure of blogs they own or on which they participate.*** Consider making it policy that if an officer starts a blog or begins to contribute to one, s/he should disclose it first. Also state your position on the prospect of posting anonymously.

• ***Email addresses.*** Applicants should provide email addresses that they have used in the past. Law

enforcement generally agrees an email address is an important search term. Issues here include the applicants memory of all email addresses, or those used for undercover or sensitive work.

• ***Disclosure of online identity.*** Many agencies are asking applicants to list current screen names and nicknames used online. What happens if they disclose bank account username/password (because it may be the same as that used for a social platform) and then something happens to that account? Or their identities are stolen. Can they come back and blame your agency?

• ***Command Performance.*** Many agencies are opting to have applicants open up their password-protected sites during the face-to-face interview so that decision makers can review online content during the face-to-face interview, sometimes without warning. Applicants should be afforded the opportunity to explain any online information.

• ***Limited to a workplace computer.*** Authorized personnel conducting Internet searches for employment or security clearance purposes may review online information from publicly accessible, unrestricted websites.

• ***Use of applicants social security number in searches.*** There are many inherent dangers to the practice of putting someone's social security number in an online search. Doing so can make it viewable to others. It isn't recommended to be done on social sites which index content.

• ***Misrepresentation.*** Circumstances under which misrepresentations will be made to obtain online information need to be defined. Besides being in potential violation of social network's terms of service, this topic is controversial. You create fake profiles to catch pedofiles, but under what conditions, if any, would you consider creating a fake profile to investigate a potential employee

• ***Wall-off.*** Some law officers have indicated they feel that if someone discloses potential protected-class types of info online it's equivalent to a waiver of their privacy. That doesn't mean a judge would agree. A wall-off procedure needs to be in place to protect the applicant and the hiring manager regarding Internet search results pertaining to protected classes (e.g., age, sexual orientation, race, etc) so that the hiring manager doesn't see information falling within the definition of protected class.

• ***Criminal Evidence.*** When/if criminal evidence is uncovered during a cyber-vetting procedure, what is done with the evidence?

4. Monitoring & Reporting After Hire (some or all of the points in this section could also fall under the "general use" section above)

• ***Ongoing monitoring.*** Employees should be informed if it is the agency's intention to monitor their activities online.

• Conditions for ongoing monitoring. In response to specific concerns, complaints, or information about an employee, organizations may conduct online searches to obtain additional information on that employee.

• ***Reporting by peers.*** Should an employee who becomes aware of an Internet posting or Web site that is in violation of the organization's policies report the information to a supervisor. Are anonymous reports o.k?

• ***Accountability.*** Employees shall be responsible for ensuring that sensitive information is not posted on their family members' social networking sites.

• ***Rebuttal/Defense.*** Employees should be given the opportunity to address anything negative found online. It could be the work of an imposter or an angry ex-spouse. Is the employee allowed to have a copy of the evidence?

5. Application of Internet vetting findings

• ***Employment decisions.*** Hiring, retention, promotion, security clearances and disciplinary decisions, based at least in part on the results of an Internet search, must be based on established criteria and processes.

• ***Security.*** How are the results of Internet searches stored and protected? For your own protection as well as that of the candidates, establish conditions under which the results of your investigation is destroy or stored, and for how long. On the one hand, you may not want it around for liability reasons, on the other if you deny employment to someone, you may need the evidence to prove your negative decision was NOT discrimination.

III. Investigations Policy

I'm not a trained investigator, but I offer a few points here only to the extent social media platforms are involved.

- ***False identities.*** Give proper consideration for the procedure by which you will obtain false identities and take into consideration the workings of each platform.
- ***Department only equipment.*** The use of department-only equipment which has no online identifiable ties to the agency. This is standard in any investigation but take special consideration for the use of mobile technology, especially geo-location enabled.
- ***Training/Competence.*** Always important. There's always a new tool, sometimes a very simple one that will benefit your agency. Keep your investigators well trained and don't underestimate the value of training by professionals who genuinely live in the world of social media. Any cyber-investigator knows how to put up a false profile, but examine whether your trainer really is up-to-date on the very latest technical developments in the social world. Include in your policy that training is to be provided and investigators need to take on responsibility to know what they don't know and learn it. A good cyber-investigator stays up to date him or herself by tuning in social media blogs and other sources.
- ***Proper documentation.*** The technique of gathering of anything online should be treated with great care. How it was obtained, with date-stamp, in the chronological order it was obtained is of upmost importance. And, with social networks, the content itself changes quickly. Evidence needs to be gathered more quickly than may have otherwise been necessary, don't lose sight of the need to document carefully.
- ***TOS violations.*** Some investigative activity is technically against the Terms of Service for social networking platforms. Know the TOS statements of the platforms you're using and put into policy under what circumstances your agency will conduct activity which may otherwise be in violation of those TOS.

Three Final Thoughts...

In addition to the specific points above, there are some themes that transcend all policy development in social media.

- ***Consistency.*** One of the biggest arguments for social media policy is so that your agency can be sure that personnel are all treated equally. If you're accused in court of discrimination in a hiring decision and you don't even have a document to present that shows you intend to perform fairly for everybody, that's a big piece of potential protection missing. Of course, actually practicing consistency goes hand in hand with saying you do so.
- ***Training/Competence.*** Training and competence are not the same. I regularly see and hear policy personnel saying training should be part of all policies. But just because training is provided, doesn't mean the trainee is competent with the tools. I recommend putting the onus on the employee to be able to assure his or her thorough knowledge of the platforms s/he is on regardless of purpose. A great majority of the cases where an officer gets himself into trouble – especially on Facebook – with career ruining activity, could have been prevented if the players had better knowledge of how the platform worked. So provide the training, but include separately that they will held accountable and that blaming mistakes on not knowing it would happen won't be tolerated.
- ***Honor your agency's culture.*** No matter what you read or who you talk to, always honor the culture of your own organization when developing policy. If your agency doesn't need to be overly restrictive and punitive with social media, especially with regard to how you expect sworn officers to behave when representing the department, you will know it. Moreover, the agency will benefit because the officers won't feel like it's just not worth doing because it's too easy to get into trouble.

It's a brave new world we live in. The main thing is to go forth without fear of these media. There's more benefit than risk and sound policy will go a long way towards protecting your agency in the online world as well as allay fears that you're not ready.

About the author

Lauri is passionate about the Internet, the web, social media and helping law enforcement leverage these tools to help them do their jobs, connect with their communities, and promote their departments. Having used the net since the mid-80s, before the web existed, makes her one of the first fraction of a 1% of people in the world on the net. She holds an