

# Law Enforcement Guide to Social Media



By ROCIC Publications Specialist Jennifer Adkins  
© 2011 ROCIC

Law enforcement agencies are increasingly developing strategies that utilize social media as investigative resources, including Facebook, Twitter, MySpace, and YouTube. Social media is a term that refers to the use of Web-based and mobile technologies that enable people to communicate easily via the Internet to share information and resources. Agencies maintain social network accounts to facilitate communication within their community, distributing information on criminal activity quickly and effectively. They are also using criminals' social accounts to track their whereabouts and actions. This information is being used to further investigations and help in prosecuting these criminals. However, law enforcement agencies should be cautious in maintaining their own social network, because wrongfully posted information (or comments made by officers on their personal social media accounts) could hinder investigations or damage the agency's reputation.

## Case Study: Police Use Facebook to Arrest Sex Predator

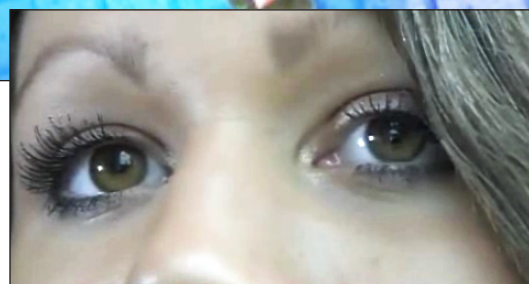


Law enforcement officers utilized Facebook, an online social network, to identify and capture a multi-state sexual predator, who used the same social network to prey on sorority sisters at universities in Florida, Louisiana, Alabama, Georgia, Mississippi, Texas, Tennessee, Ohio, and Missouri.

From October to November, 2010, an unidentified suspect, posing as a sorority sister named Lexie Hillbrenner, instructed the females to take off their clothing and perform various acts in order to pledge into an alleged sorority. He utilized four fake Facebook social network accounts to contact sorority pledges. Once the student realized the contact was a hoax, the suspect would continue his demands, threatening to post naked pictures of the student on the Internet.

He had 12 conversations with one victim, each one becoming more and more invasive. The suspect asked the victim what kind of underwear she was wearing, and asked her to ball it up and put it in her mouth. The victim originally assumed the requests were part of a pledge ritual. When she discovered that he was a predator, she contacted police.

Similar cases were reported at Louisiana State University, the University of Florida, the University of Central Florida in Orlando, the University of Georgia, the University of



Alabama, the University of Mississippi, Miami (Ohio) University, Texas-Tech University, the University of Tennessee in Knoxville, and the University of Missouri.

Investigators at Florida State University, Louisiana State University, Auburn University, and the Florida Department of Law Enforcement began comparing notes and contacted Facebook for help. LSU officers also utilized the ROCIC Bulletin to identify other similar cases.

An LSU detective was able to subpoena an IP address to three separate locations, two in Key West, Fla., and one in Cincinnati, Ohio. Subsequently, LSU Police, the FDLE, and a cybercrime contact with Facebook identified 20 alias accounts belonging to Mitchell W. Hill. (An IP address is similar to a fingerprint that identifies a particular computer.)

On Dec. 10, 2010, Hill was arrested on a Louisiana warrant in Key West, Fla., where police seized a computer linked to the online harassment of 11 female victims. He was charged with video voyeurism, extortion, and attempted video voyeurism.

## **Technology and the Modern Policing Strategy**

Law enforcement agencies are increasingly using social networking Web sites as crime-fighting tools. However, navigating social media sites poses new challenges to officers.

Social media should be part of a modern policing strategy, which allows officers to stay ahead of criminals. Law enforcement is now using Facebook, MySpace, Twitter, and YouTube during every step of an investigation, making their jobs easier because they have access to instant information. Social media also makes the public's efforts to combat crime more effective.

Citizens are vulnerable to criminals due to online social networking, causing officers to have to reach out further to their communities. The click of a mouse allows photos of criminals to be disseminated throughout the community within a second. Agencies are now maintaining crime-tip email accounts, Twitter accounts, and Facebook pages.

Agencies' social media pages are also used to communicate with the public, and provide crime alerts, weather updates, and major emergency information online. In addition, some departments are using social networking to communicate with journalists, such as posting a news release to their Facebook page.

Although there are many advantages, there are challenges as well. Comments on personal sites can have significant implications and can damage cases being investigated. Agencies should establish policies for the use of the agency's site and personal sites. It is important to educate officers on safety issues regarding social media.

### **Social Media Laws**

The use of social networking as evidence is so new that there isn't much existing case law for judges to refer to; however, the implications of using social networking sites during a trial is boundless.

For example, prosecutors working to convict Jared Loughner, the alleged gunman who shot Representative Gabrielle Giffords on Jan. 8, 2011, may use the "goodbye friends" message he wrote on MySpace just prior to the shooting in Arizona.

In June 2010, Jason Isbell was convicted of killing a passenger during a drunk driving crash in Lake Wylie, S.C. The prosecution showed the jury Facebook pictures of the defendant partying and drinking at bars in Tennessee. Police can use similar posted information to get a confession.

### **The Threat of Geotagging on Social Network Sites**

Geotagging is a feature on smartphones that geographically tags the location and time of a photograph taken. When that photograph is uploaded to a social Web site, the information is a few clicks away with the right browser software. This geographic information poses serious threats to citizens. For instance, if a mother takes a picture of her young daughter in her bedroom, and posts it to Facebook or Twitter, a sex offender could potentially find her daughter's bedroom. Approximately 76 percent of American adults use their mobile devices to take pictures or videos, according to a Pew Research Report.

Geotagging can add geographical information to photographs, video, Web sites, SMS messages, RSS feeds, or tweets. Social networkers can now not only read what their friends are doing, but where they are. Social networking sites offer privacy options for the geotagging feature. Facebook allows users to limit who sees their location, and Twitter has the option of turning on or off "adding your location" to a tweet.

Using Google Maps, a person's whereabouts and path can be tracked using the metadata encoded in photographs taken, as long as the GPS is enabled when taking the picture with the phone or the geotagging tool is enabled in photo settings. Law enforcement can use the same information to track down criminals and determine a timeline for various crimes.

## **Criminals “Tagged”: Using Facebook as an Investigative Tool**

### **What is Facebook?**

Facebook is a major social networking Web site that allows anyone over the age of 13 with a valid email address to become a user. Facebook markets itself as a way to connect and share with people in your life. In 2010, there were an estimated 149 million active users on Facebook.

Users can create profiles with photos, contact information, lists of personal interests, lists of personal contacts, and other personal information. They communicate with their friends through public or private messages. Facebook rules specify that users give their real identity (unlike MySpace). Users can update their statuses to inform their friends (or anyone else viewing the profile) of their whereabouts and actions.

### **Facebook Helps Fight Crime, Collect Evidence**

Using social networking in criminal cases can reveal a suspect's whereabouts, establish motives, personal relations, and prove or disprove alibis. If the information is public, law enforcement can view it and use it.

Law enforcement can also take measures to retrieve private data with a warrant or subpoena. Facebook has been cooperative regarding emergency law enforcement measures, such as with a kidnapped child; however, a minimum amount of information is shared.

MySpace has created a law enforcement guide (posted on the interactive version of this report on the ROCIC Web site), and developed a 24/7 hotline and an email account to assist investigations. MySpace requires a search warrant to view private messages less than 181 days old.

Law enforcement and ROCIC can use social networking sites to search for evidence and witnesses in criminal cases, and in some instances, track suspects. In fact, some law enforcement officers have created fake personalities on Facebook in order to befriend suspects and gain information, similar to law enforcement agencies using online

chat rooms to lure child pornography traffickers and sex predators.

Law enforcement can also examine photos posted on Facebook for evidence of participation in a crime. For instance, if a person is suspected of participating in a robbery, the investigating officer could look at recently posted pictures for jewelry, guns, or other evidence. In addition, friend lists can yield witnesses or informants. Facebook is also a resource for locating next-of-kin.

### **Case Studies**

In June 2011, Facebook led Danielsville, Ga. officers to a burglary suspect in Madison County, Ga. The Danielsville Sheriff's Office posted a picture of the suspect on the agency's Facebook page and received a tip that the suspect was at his residence in Madison County. He was arrested without incident. Two days earlier, two other burglars were arrested based on tips received through Facebook.

In March 2011, a missing Tucson, Ariz. juvenile female was reunited with her family after her relationship with a 19-year-old was tracked through Facebook and led authorities to Texas.

In November 2010, an inmate and member of the Aryan Brotherhood serving a 30-year murder sentence in Tulsa, Okla. (convicted of killing a sheriff) posted several pictures on his Facebook profile from jail exhibiting various illicit items, including marijuana joints, alcohol, and weapons. He used a contraband cell phone to post the pictures. Possessing a cell phone in prison is a felony. The suspect was moved to a maximum-security penitentiary and segregated from other inmates.

In August 2009, a burglar was arrested after he checked his Facebook account on the victim's computer (and forgot to log out) before stealing two diamond rings. The victim discovered his account was still open on her computer. A friend of the victim advised police where the burglar resided. The suspect was located and arrested.

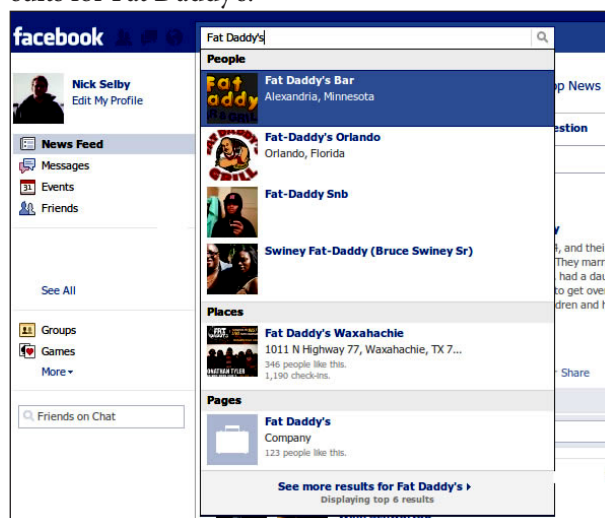


## Facebook Search Tips for Officers & Law Enforcement Analysts

The Facebook search bar is a powerful tool for law enforcement. All public conversations are accessible to law enforcement (the officer should first be registered). The following example is from a Police-Led Intelligence article, and shows how to search for people talking about a bar called Fat Daddy's.

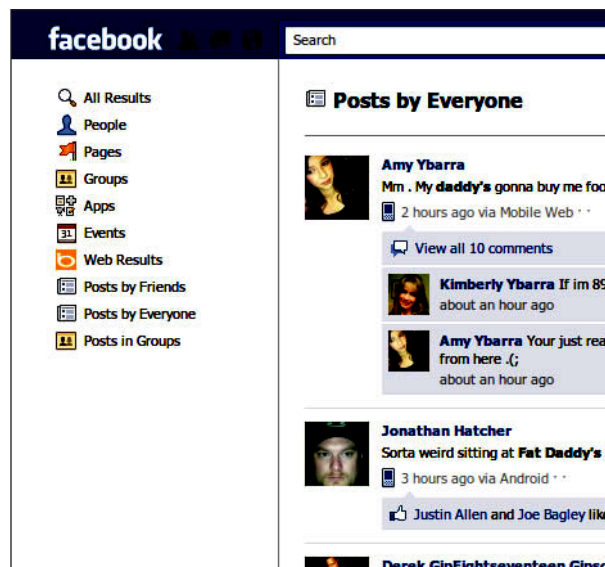
### Step One

Type in Fat Daddy's in the search bar, located to the right of the Facebook logo. Ignore all titles that pop up. At the bottom of the list, click on "See More Results for Fat Daddy's."



### Step Two

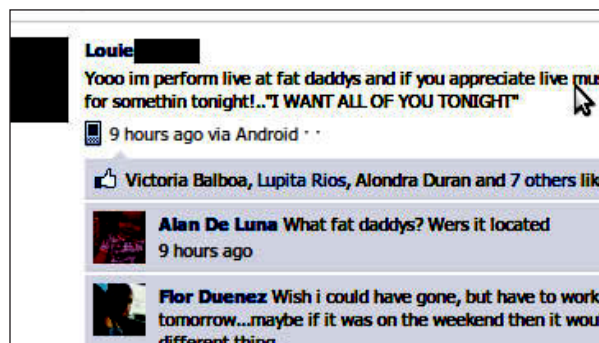
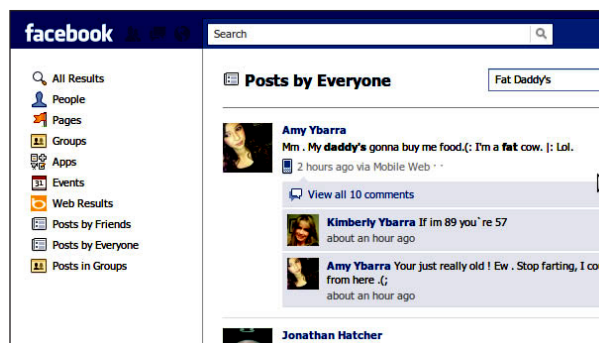
Click on "Posts By Everyone" located in the links to the left of the main content.



### Step Three

The resultant page is a real-time list of conversations including the search term (top right picture). The posts will also include just the words "Fat," and "Daddy's." Adding double quotes around the search phrase will limit the results to just that phrase.

If an investigator was looking for a person named Louie who frequents Fat Daddy's in Fort Worth, that investigator may see him discussing his impending visit tonight, even if he is not the investigator's Facebook friend.



If the Facebook search bar is too time-consuming, they can also utilize openstatussearch.com and type the search term into their search box. They search public timeline posts without logging into Facebook.

In addition, officers can also search for suspects by going to [www.pipl.com](http://www.pipl.com), a comprehensive people search on the Internet. Pipl Web site searches personal profiles, public records, and other people-related documents stored in databases, not on Web pages. These pages are invisible to regular search engines.

## **Tweets from the Streets: Using Twitter as a Law Enforcement Tool**

### **What is Twitter?**

Twitter is a social network that enables users to send messages to other users. These messages are known as tweets, a text-based post of up to 140 characters displayed on the user's profile page, and essentially updates other users on the poster's whereabouts and actions.

Approximately 200 million tweets are sent daily. Tweets are public by default; however, senders can restrict message delivery to just their followers. A Twitter user becomes a follower by requesting to be alerted when another user posts a new message. Followers are also known as tweeps (peeps or pals).

Twitter allows users to update their profile via their cell phone either by text message or apps installed on certain smartphones. When a person tweets, the message is visible on all the profiles of that person's followers. The followers can then retweet (repost) the message to their own followers. The messages are organized on the Twitter user's profile page by topic. Twitter was ranked the fastest-growing Web site in 2009, followed by Zimbio (a magazine publishing Web site) and Facebook.

### **Using Twitter as an Investigative Tool**

Social network technologies are transforming our culture and also changing how law enforcement does business. Law enforcement can detect threats earlier, and respond quicker and better.

Similar to Facebook, officers can utilize Twitter to send out tweets about crimes committed in their jurisdictions and receive tips from the community. Twitter is a way for officers to get important information on crime out to their communities so that citizens can take measures to protect themselves.

Twitter can also be utilized to provide updates on road closures, ongoing incidents that affect the community, and in cases (such as natural disasters) when the public and media need to be notified immediately.

### **Tactical Tweeting ([www.TACTweet.com](http://www.TACTweet.com))**

Tactical Tweeting (TacTweet) is a free Web service, designed by Global Technology Solutions, that enables law enforcement officers to anonymously monitor open-source tweets worldwide. It was designed by former special agents and law enforcement experts to securely tap into social networks data and information for actionable intelligence.

The site helps officers monitor, collect, and analyze tweets to alert them to emergencies and crimes, accelerating the speed by which officers respond to emerging threats and cutting down on costs of equipment.

Officers can monitor drug deals and other types of crimes by typing keywords into TacTweet. For instance, during a Social Media Conference hosted by IBM officials to educate law enforcement officers in Atlanta, Ga. on using social networks as investigative tools, an officer typed in the keyword "weed." Within seconds, lists of tweets involving illegal marijuana distribution were located on Twitter. The officers could see who posted the tweet, and who follows the tweeter. Within a minute, the officers uncovered a criminal network of people buying and selling illegal marijuana.

Officers can also use TacTweet during states of emergency by using a feature known as a mashup. A technology mashup is an application that combines data and information from two or more sources and presents the information in an understandable way. By mashing data from various social networks, a law enforcement agency can improve its intelligence collection and situational awareness.

Officers can access these mashups through keywords on TacTweet. For instance, if a school went into a lockdown because a gunman is roaming the hallways, people can immediately send tweets to family members and friends alerting them of the lockdown. If officers are monitoring tweets, they can type in the keyword "lockdown" and receive all the information sent.

### Case Studies

In May 2011, Tampa, Fla. police learned about a 24-year-old woman's rape after she posted it on Twitter. The woman was living in a renovated school bus, and a black male suspect with a scruffy beard broke into the vehicle and sexually assaulted her. Officers took steps to protect the victim, and began searching for the suspect. Police requested she quit tweeting about the incident as it could hinder the investigation.

On April 19, 2011, Dunwoody, Ga. police spent the day tweeting every move they made in an effort to show their community exactly what officers go through each day, and to gain more followers. Most of the tweets were routine traffic stops, but others were more interesting. A two-car accident turned into a felony arrest after the officer on the scene realized one of the drivers was wanted on drug charges.

In March 2011, a 25-year-old former high school assistant coach in Lake Saint Louis, Miss. was sentenced to seven years in prison after he violated his probation by using Twitter. He was sentenced to probation after being convicted of having sex with a 16-year-old female student on the condition he did not use social networking sites. The day after he was sentenced, the suspect posted tweets criticizing the judge, who had agreed to the probation.

In 2008, students at the University of Central Oklahoma bragged on MySpace and Twitter that their party business had served thousands, a boast that allowed the Oklahoma Tax Commission to issue a six-figure state tax bill. The IRS uses Twitter, Facebook, and Google Street Map to collect information for investigations on tax cheats. The IRS also provides news feeds via Twitter, providing tax news and information for taxpayers.

## Twitter Search Tips for Officers & Law Enforcement Analysts

To find whether someone is on Twitter, go to the Who To Follow Web page, which works even if you are logged out. The following example is from a Police-Led Intelligence article, and shows how to conduct a search for a person named Nick Selby.



To find out whether Nick Selby talked about something specific, go to the Twitter Advanced Search. Type in keywords, and view what Nick Selby has said about each keyword. If an investigator types these keywords into the regular search engines, using quotes, he or she would receive the same results ("shotspotter" or "co-dependent" or "car talk" from:nSelby).

Advanced Search Results offer options to search conversations from and to people, and there are geographical options. Searching attitudes may also give evidence of intent.

A screenshot of the Twitter Advanced Search form. It is organized into several sections: 'People' with fields for 'From this person' (containing 'nSelby'), 'To this person', and 'Referencing this person'; 'Places' with fields for 'Near this place' and 'Within this distance' (set to 15 miles); 'Dates' with fields for 'Since this date' and 'Until this date'; and 'Attitudes' with checkboxes for 'With positive attitude :)', 'With negative attitude :( ', and 'Asking a question ?'. There are also radio buttons for 'miles' and 'kilo' in the 'Within this distance' field.

## Thugs, Drugs, and Social Networks

The Lee County, Fla. Sheriff's Office arrested 15 suspected gang members after viewing the contents of their MySpace pages, which prosecutors claimed advertised and promoted gang membership. These were the first arrests after the passing of a 2009 Florida law that criminalized the promotion of gangs on the Internet. Violators face a maximum five years in prison.



Gang communication has changed with technology, and, like the rest of the world, has gone online. There is an increasing use of social networking sites like Facebook and Twitter to organize criminal activities and threaten rival gangs. Officers are now using social network profiles to conduct gang-related investigations, and to identify gang affiliations. Prosecutors are also using photos obtained from social networks to prove to the jury a gang member's image, affiliation, and past actions.

Gang members like to publicize themselves on the Internet. They pose with weapons, gang signs, and gang colors and post the pictures on their social Web pages, as well as post rap videos on YouTube. Some gang members have been caught with stolen money or guns, or show videos of themselves with vehicles identified as involved in a crime.

Gangs are also turning to Twitter and other social media sites to recruit members, broaden their appeal, make threats, and boast of their exploits. Gangs use social networking sites to circumvent court injunctions that forbid gang members meeting in public.

Gang members can now victimize specific individuals, and track their whereabouts using geotagging. They can also target victims by creating false

identities and accounts. Adolescents visiting social networking sites to download music and pictures that glorify criminal street gangs can unwittingly set themselves up to be recruited by gangs.

Law enforcement should monitor photographs, tweets, social linkages, and social events posted publicly on Web sites to identify and track suspect criminals. In one case, a suspect was wanted for felony theft and captured after posting on Twitter that he would be hosting his birthday party at a specific time and place.

Officers can use IP addresses at nondescript locations (public library or local college) to make it more difficult for suspects to detect their computer activity being tracked by police. In addition, ROCIC offers various anonymizers through RISSNet, that anonymizes the officer's IP address.

Law enforcement should include all electronic devices in their search warrants, as well as keep files and hard copies of all information gathered online. Back up files on portable hard drives. If evidence online is located, it is a good idea to do a dated screen-capture of the Web page and save it.

In the past, Facebook and other networking sites have been cooperative when records have been subpoenaed for the courts. However, the Web sites almost always require that they be subpoenaed.



## ROCIC Utilizes Social Networks to Assist Investigations

The ROCIC Criminal Intelligence Unit uses its profiles to view suspects' pages, images, and information. In addition, the CIU can access Facebook, Twitter, MySpace, YouTube, and other social networking sites to look for information, including:

- Place of Employment
- Last Known Addresses
- Photos
- Friends and Affiliates
- Whereabouts/Actions on Dates of Interest
- Incriminating Comments

Criminal Intelligence Analysts can also provide officers with screen captures of a suspect's social network pages, photos, and other items of interest. Many law enforcement agencies do not have access to this information because of firewall issues. Analysts also perform image and video Internet searches on social networking sites to find information on a particular:

- Gang Name
- Tattoo (meaning of a tattoo)
- Person's Name
- Trend
- Nickname (meaning of a nickname)

This information is useful in cases involving juveniles – where a credit or address history does not exist. In addition, officers can utilize RISSLeads to search for current investigative resources regarding social networking postings.



### Postal inspectors use ROCIC to locate multi-state fraud suspect

The ROCIC Criminal Intelligence Unit ran Facebook inquiries on a subject under investigation by the U.S. Postal Inspection Service in Charlotte, N.C., which used information on the subject's boyfriend's Facebook page to generate an address in Georgia where the suspect was subsequently located and arrested. The suspect had been passing counterfeit USPS money orders throughout the U.S. under false identities.

POST REFRESH SEARCH MARK READ MORE HELP LOGOFF

SHOW CHAT HIDE CHAT CHAT LIST

**RISSLeads Conferences**

All Messages | [135 New](#) | [0 Attn](#)

[RISSGang Website](#) [RISSGang BB](#)

Welcome to RISSLeads

- \*Ask The Admin (1)
- \*RISSLeads User Tips (11)
- \*Test (only) (0)
- \*Critical (BOLOs & Officer Safety) (21, 1 New) **New**
- \*Members Forum (48, 2 New) **New**
- \*Request For Information (RFI) (159, 1 New) **New**
- \*INVESTIGATIVE RESOURCES (1)
- \*Investigative Resources 2006 (20)
- \*Investigative Resources 2007 (45)
- \*Investigative Resources 2008 (83)
- \*Investigative Resources 2009 (140)
- \*Investigative Resources 2010 (237)
- \*Investigative Resources 2011 (148, 2 New) **New**

Today's Messages | [Search Messages](#)

Message search results for **social**

Found 7 Messages.

Conference	Topic	Date
1 *Investigative Resources 2011	<a href="#">Thin Blue Link (Social Networking Web...</a>	6/14/
2 *Investigative Resources 2011	<a href="#">OPSEC - SAFE Social Networking</a>	2/22/
3 *Investigative Resources 2011	<a href="#">OPSEC, Social Networking Sites,</a>	2/18/
4 *Investigative Resources 2011	<a href="#">Use of Social Networking Sites Target...</a>	1/12/
5 *Investigative Resources 2011	<a href="#">Spokeo social network</a>	1/11/
6 *Investigative Resources 2011	<a href="#">The E-Verify Program</a>	1/10/
7 *Investigative Resources 2011	<a href="#">USArmy - Geotag &amp; Location-Based Sod...</a>	1/10/

## Using Social Media to Inform the Community

Social media has transformed the relationship between law enforcement and citizens. Social networks allow citizens to check and hear what is going on in their community, directly from the police. Agencies are also posting pictures of criminals and receiving feedback and tips from civilians. Social networks give officers the chance to address the concerns of their community.

It is critical that law enforcement officers use social networking to enhance their reputations and maintain a positive image. Agencies should establish clear policies on how officers should conduct themselves on social Web sites (e.g. not discussing pending cases).

Tuscaloosa County, Ala. Sheriff's Office uses Facebook and Twitter accounts to provide crime alerts, weather updates, and other information online.

### Managing Agencies' Social Media

The International Association of Chiefs of Police (IACP) Center for Social Media breaks down the development process of creating a social media presence into four actions: **defining social media, strategy development, policy development, and putting it into action.**

There are ten key strategy considerations when developing a social media strategy, according to IACP:

1. **Research.** Researching promising practices and social media use in law enforcement can be helpful in providing insight and direction concerning your own strategy. Research may also include what platforms your community members are using, how are they using them, and what are they saying about your agency.
2. **Management.** Determine who will manage your social media presence. Will this person be responsible for creating and publishing the content to your social media sites? It is important to consider this early on to ensure key stakeholders are involved in the planning process. Keep in mind social media tools are modes of com-

munication, and are best placed in the hands of those familiar with communication and outreach strategies.

3. **Fears.** What fears do you have related to social media? Acknowledge these fears and determine how you will move forward in a manner that is conscientious of these concerns.
4. **Goals.** As with any new initiative, it is important to set goals. Your goals may be diverse, ranging from strictly numerical outputs such as page views or number of followers, to offline behaviors and actions, to overarching community themes such as reduced crime or improved police-community relations. Some of these goals may seem difficult to measure, but identify them anyway.
5. **Audience.** Identify your current audience as well as potential audiences that you may not be reaching or audiences you hope to reach in the future. Social media will allow you to reach a broad audience and include new demographics in your outreach.
6. **Content.** The content you share may include news, event information, disaster preparedness tips, and alerts. Your goals will help determine the types of content you choose to distribute. Keep in mind that social media outlets do not limit you to text; consider using other types of content such as pictures and video.
7. **Level of Engagement.** Your goals will also help determine the degree of interaction you want to facilitate. Social media sites promote user participation; however, as you set up your presence on various platforms you have the option of restricting certain types of interaction (e.g. user comments).
8. **Platforms.** Your answers to type of content, level of engagement, and audience in combination with your goals and research will help to determine the platform or platforms that best suit your needs. Different social media platforms

provide different modes for communicating and have different demographic representation.

9. **Integration.** Remember, social media is just one tool that will help to enhance your communication and outreach initiatives. Social media can work within your current framework and is not meant as a substitute for other tools and methods.

10. **Follow-up.** Is your strategy working for you? What about your community? Look back to the goals you set and establish if you are meeting those goals or have put yourself on track to meet those goals. If not, determine what needs to change. Social media is flexible and ever changing and allows you to generate the experience that best suits your agency and your community.

Policy development should consider and address technology and legal issues concerning the functions of the law enforcement agency. It is important to review the policy with the legal and communications department of your agency. Five key policy considerations include:

1. **Scope.** Determine what areas the policy needs to cover. Once the scope is determined, consider the areas below that apply to the areas you have chosen to cover in your policy.
2. **Official Use.** Social media tools can be used for many purposes and are valuable for many day-to-day operational activities in law enforcement agencies. It is integral that authorization for and administration of any department-sanctioned sites are clearly articulated.
3. **Personal Use.** Content posted by law enforcement, even off-duty and under strict privacy set-



tings, has the potential to be disseminated broadly and fall into the hands of defense attorneys, criminals, and members of the community. Any improper postings can ultimately affect an individual's credibility, employment status, and their agency as a whole.

4. **Legal Issues.** Issues such as First Amendment rights, records retention and public records laws, and other federal and state statutes must be considered while crafting a policy. Many legal issues surrounding social media have not yet been settled within the court system, so having clear guidelines in place becomes even more imperative.
5. **Related Policies.** Many issues surrounding social media use may be resolved by citing other policies that are already in place within your agency, including Internet Use, Electronic Messaging, Code of Conduct, and Media Relations. The IACP's National Law Enforcement Policy Center offers model policies on these topics.

After the strategies and policies are developed and the management is in place, they are ready to be put into action. The IACP offers numerous resources and videos in helping to maintain an agency's social network.

**Blog Post by Mark Economou, Public Information Officer  
for the Boca Raton, Fla. P.D.'s Social Media Management**

“One of the top questions I get from agencies around the country exploring the possibility of using social media is how much time does it take? That question usually leads to another, like how many people manage it? Others don’t think they have the resources to handle it. I tell all agencies, any department no matter how big or small can have employees on staff that can handle social media.

Most agencies have a Web site. Most agencies have someone who writes their releases. If that’s the case, then most have the ability to manage social media. Here in Boca Raton, I handle the bulk of the social media management. Throughout the day, I sign on to Facebook and check for comments or questions. For Twitter, I leave TweetDeck open on my computer and check in throughout the day. If there are new press releases or articles to put on our Web page, I take the extra five minutes to also post on Facebook and tweet it out.

One of the problems for most agencies is managing the social media accounts after hours or on weekends. This is a continuing concern for many. We, right up front on our sites, have a disclaimer basically saying the social media sites are not monitored 24/7 and any and all crime-related issues should be directed to 911 or our dispatch center. With the advent of smart phones it does make it easier to manage those accounts after hours. With a couple of touches of the screen on my phone I can see if anyone posted or commented on anything. If not, no time lost; if they did, I respond. Again, hardly any time taken.

Social media management is not as difficult as most think. It does take someone who is computer and Internet savvy, and it does help to have someone who knows and likes social media.

Just make sure if you are posting a comment you have the correct account open. Nothing would be more embarrassing than making a comment you thought was on your personal page but was sent over your agency site. More on that at a later date.”





### **Social Media Search Engines**

#### **Kurrently**

Kurrently is a search engine launched in 2010 that offers the ability to search Facebook and Twitter in real time. It combines results from the social networks in a fast format. The results are organized by date and update as the list is viewed.

#### **IP-Address**

Ip-adress.com/ip\_tracer allows users to find the IP address of emailers, showing the location from where the message was sent.

#### **PasteLert**

PasteLert searches pastebin.com and sets up alerts sent to your email when your previous searches are found in new pastebin entries. Pastebin allows users to upload snippets of text from social media sites or other sources for public viewing.

#### **Pipl**

Pipl is a comprehensive people search on the Internet. Pipl searches a part of the Internet known as the deep web, which refers to a repository of underlying content that general search engines (such as Google) can't reach. The results come from documents in online databases.

#### **Social Mention**

Social Mention searches user-generated content such as blogs, comments, bookmarks, events, news, videos and others. It sends alerts to your email based on your previous searches.

#### **TweetGrid**

TweetGrid is a real-time Twitter search engine that allows you to search for up to nine different topics, events, conversations, hashtags (Twitter shorthand), phrases, people, groups, and, notably, photos posted on Twitter.

#### **Who's Talkin**

Who's Talkin is a search engine that searches for conversations about topics of interest. The results are a combination of data taken from more than 60 social media sites. The results are given in a well-organized format.

## **Other Social Media Sources Utilized by Officers Worldwide**

### **Collier County, Fla. Sheriff's Office**

The Collier County Sheriff's Office launched CCSO2go, an iPhone app that gives users an array of CCSO news and safety information. CCSO is among many law enforcement agencies that now offer their own iPhone app. It allows users to find out who has been arrested, to obtain real-time traffic information, and to help map out their commutes. They can also connect to the agency's Facebook and Twitter feeds, get directions, watch CCSO videos on YouTube, and call the CCSO substation. The app is available at iTunes App Store.

### **Barrie, Canada Police Department**

The Barrie Police Department uses a Google-based mapping feature on the department's Web site to show a neighborhood crime report, which shows what crimes have happened and where. Crimes include robbery, breaking and entering, and stolen vehicles. The feature also provides statistics to the community and shares the data with neighborhood watch groups. The statistics represent crime occurring within the past two months.

### **Jackson County, Mich. Sheriff's Office**

Jackson County Sheriff's Office has started to experiment with quick response codes (QR codes), which are similar to bar codes and readable by smartphones. The codes were designed to take people to Web sites with more information about products or services. A QR code was developed for the sheriff's office, so that when scanned, it takes people to the department's Web site. The codes may be placed on signs outside the department's office, jail, and possibly on patrol cars.

### **Ventura County, Calif. Sheriff's Department**

The Ventura County Sheriff's Department uses Nixle, a site that allows agencies to post information directly onto an online platform. Staffers can then share the link via Twitter, allowing the public to read a news release sent out by the department. Nixle posts are available through cell phones, email and computers, and the posts can also be seen on the department's Web site.

## Negative Career Implications Due to Social Networking

Facebook and social networking activity of law enforcement officers has negatively impacted the careers and reputations of several officers throughout the country. Here are just a few examples:

- A Sandy Spring, Ga. officer was fired after he posted specific information about a raid that the police would be executing.
- A South Carolina police officer was fired after a photo surfaced on Facebook of scantily-clad women posing on the hood of his town police cruiser.
- A Shannon Hills, Ark. officer was terminated after he posted information jeopardizing a DUI checkpoint, information which violated the Shannon Hills department's code of ethics.
- An officer's credibility on the stand was attacked by the defense using a status update from his Facebook page. The defense attorney used this information to paint the officer as over-zealous. The defense attorney later stated that the officer



*Three officers in New York were suspended after posting inappropriate comments on Facebook.*

was “motivated to cover up his use of excessive force” and that the Facebook comments support that.

For information regarding setting your privacy settings, sharing on Facebook, directory information, and status updates/wall posts, consult the Law Enforcement Facebook Privacy Guide posted on the interactive version of this report at [rocic.riss.net/Publications](http://rocic.riss.net/Publications).

## Sources of Information

### 2010 Law Enforcement Training Conference

ROCIC Training Conference Report  
[rocic.riss.net/publications.htm](http://rocic.riss.net/publications.htm)

### IACP Center for Social Media

Multiple Articles  
[www.iacpsocialmedia.org](http://www.iacpsocialmedia.org)

### Facebook

[www.facebook.com](http://www.facebook.com)

### Law Enforcement Facebook Privacy Guide

[www.lvpmsa.org](http://www.lvpmsa.org)

### Police-Led Intelligence

Social Media Search Tips for Cops & Law Enforcement Analysts  
[policeledintelligence.com](http://policeledintelligence.com)

### Twitter

[www.twitter.com](http://www.twitter.com)

### Warner, Richard

Podcast: Using Twitter to fight Crime  
[www.whatsupinteractive.com](http://www.whatsupinteractive.com)

Various News Articles

# Special Research Reports by ROCIC Publications

Accessible to RISS member agencies on the ROCIC secure Intranet Web site. Complete listing of ROCIC Bulletins, Special Research Reports, User's Guides, and Training Conference Reports at <http://rocic.riss.net/publications.htm>

- Bath Salts: Deadly New Designer Drug
- Marijuana Legalization: Law Enforcement's Response
- Take Back Bad Medicine! Planning, Executing, and Enhancing Prescription Drug Programs
- Sovereign Citizen Movement: Extremists Claim to be Beyond the Law
- Puppy Mills: Law Enforcement, Investigation, and Prosecution
- Law Enforcement Guide to International Names
- Church Crime: Protecting Our Houses of Worship
- Hydrogen Sulfide Suicide: Latest Technique Hazardous to First Responders and the Public
- Internet Cafe Gaming: Legal Fun or Illegal Gambling?
- Taken! Investigating Drug-Related and Financial Kidnappings
- Police Interviews: The Truth About Lies
- Hispanic Counterfeit Check Fraud
- NMVTIS: New Resource for Recovering Stolen Vehicles
- Media Relations: Maximizing Law Enforcement's Positive Image
- Moorish Nation: Sovereign Citizen Movement
- ROCIC Services Resource Guide: What Can ROCIC Do For You?
- Prescription Drug Abuse: Unsafe, Illegal, and Escalating
- Moonshine: On the Rise?
- ROCIC Gang Report 2009
- Suicide Bombers: Law Enforcement Preparing for the Worst Scenario
- 287(g) Immigration Authority for State and Local Agencies
- Gang Prevention Programs: Law Enforcement and Community Working Together
- U.S.-Mexican Border Violence
- Get Smart! with Intelligence-Led Policing
- Cargo Theft
- Contraband Cigarettes
- School Administrators Guide to Gang Prevention and Intervention
- Interpol: How the International Policing Organization Can Benefit Local Law Enforcement
- National Socialist Movement and the Neo-Nazi Threat in America: NSM Hate Group Growing in Popularity
- Law Enforcement Guide to Dogfighting
- Indoor Marijuana Grows
- New Trends in Drug Abuse: Fentanyl, Cheese, Meth Labs, Flavored Meth, Marijuana Gumballs, Chronic Candy, Budder, Popcorn, Syrup, Cocaine Coconuts
- RISSGang Resource Guide
- Pandemic: How Law Enforcement Can Fight the Upcoming Global Plague
- Jihad: The History of Islamic Terrorism
- Genuine or Fake? Law Enforcement Guide to Counterfeit Merchandise
- Online Communities Abused by Predators, Gangs
- The International Driver's Permit and the Myth of the International Driver's License
- Auto Theft in the 21st Century
- Inside the Infamous Tennessee Pot Cave
- Crowd Control: Dynamics, Psychology, Law Enforcement Tactics
- Jamaat ul-Fuqra: Gilani Followers Conducting Paramilitary Training in U.S.
- Khat: Trafficking in Foreign Plant Linked to Terrorist Financing
- Active Shooter: Protecting the Lives of Innocents in Shooting Situations
- Terrorism Threat Assessment for Large Facilities
- Check 21: New Banking Technology Challenges Law Enforcement
- ICE: Crystal Methamphetamine: Imported High-Purity Meth Replacing Domestic Lab Output
- Meth Lab Safety Issues: How to Protect Law Enforcement, First Responders, and the General Public from the Dangers of Clandestine Methamphetamine Labs
- CERT (Community Emergency Response Team): Civilian Support for First Responders
- Taxing Illegal Drugs: States Attacking Profit Motive of Dealers
- Diplomatic Immunity: Rules of Engagement for Law Enforcement
- Violence Against Law Enforcement: Law Enforcement Officers Murdered, Accidentally Killed, Assaulted in the Line of Duty
- Mara Salvatrucha (MS-13): Violent Street Gang with Military Background
- Indicators of Terrorist Activity: Stopping the Next Attack in the Planning Stages
- Internet Fraud: Techniques Used to Scam Online Consumers
- DXM: Teens Abusing Cough Medicine Risk Brain Damage, Death
- RISS Activity Report for G-8 Summit
- Mail Center Security
- Safety & Security for Electrical Infrastructure: Protecting Law Enforcement and the Public in Emergency Situations
- Crisis Response Report: Terrorist Attacks & Natural Disasters
- Eco Terrorism: Extremists Pose Domestic Threat
- Cold Case Units: Turning up the Heat
- Gypsies and Travelers
- User's Guide to ATIX

**ROCIC has been serving** its criminal justice members since 1973, and served as the prototype for the modern RISS (Regional Information Sharing Systems) Centers.

ROCIC serves more than 180,000 sworn personnel in over 2,000 criminal justice agencies located in 14 southeastern and southwestern states, Puerto Rico, and the U.S. Virgin Islands.

ROCIC provides a variety of services, free of charge, to its criminal justice member agencies:

- Centralized law enforcement databases with connectivity among law enforcement agencies and the RISS Centers using the RISS Nationwide Intelligence Network.
- Analytical processing of criminal intelligence, including phone tolls and document sorts
- Loaning of specialized, high-tech surveillance

equipment and vehicles

- Publications, including criminal intelligence bulletin
- Specialized training and membership & information exchange
- Use of investigative funds
- On-site personal assistance by law enforcement coordinators



© 2011 ROCIC • This publication was supported by Grant No. 2008-RS-CX-K005, awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. The Office of Justice Programs also coordinates the activities of the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency, and the Office for Victims of Crime. This document was prepared under the leadership, guidance and funding of the Bureau of Justice Assistance (BJA), Office of Justice Programs, U.S. Department of Justice in collaboration with the Regional Organized Crime Information Center (ROCIC). The opinions, findings, and conclusions or recommendations expressed in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice. Regional Organized Crime Information Center and ROCIC are protected by copyright laws.

