

# No Safety

## Behind the Screen

Madisonville police blaze a trail  
in emphasizing education, safety  
and accountability in social  
networking and mobile technology

ABBIE DARST | PROGRAM COORDINATOR



A young woman in Madisonville had finally made it where she wanted to be. She went to college, graduated and landed an interview for a position that was right up her alley. With her credentials and confidence, she secured her dream job in a field for which she trained. A sense of accomplishment flooded her as she celebrated having arrived in this position. But a short time later, the excitement and celebration still fresh, she received a call that threatened her confidence, her sense of security and the very position she worked so hard to obtain.

Her boss's voice echoed through her mind as he told her about a yellow envelope that landed on his desk that morning full of pictures of her in compromising situations, and he asked her why he received this package. She couldn't believe her eyes, as nude pictures from her college days flashed before her — some pictures she never knew existed and others she never expected to see again.

Her boss decided that terminating her employment was his only option, in light of these embarrassing finds.

"What do you do when, as a law enforcement officer, you get the call that says, 'I have some photos that have shown up and surfaced of me and shown to my boss,'" Madisonville Sgt. Robert Carter asked. "Could that have cost someone everything they were going for? Absolutely. Because a moment of trust in the past has turned out to be a total separation in the future.

"When you deal with individuals, your heart goes out when you see situations that could have been prevented, but it all goes back to an individuals' level of responsibility and their own individual choice," Carter continued. "People have to control themselves and kids have to make sure they understand the consequences of what they are doing."

Today's officers are policing in a world of ever-changing technology and never-ending opportunities for people to share information, pictures and videos across a variety of social-networking sites and mobile networks. The task of educating themselves and the public to the potential dangers of this technology is pertinent and necessary.

The Madisonville Police Department has taken this task of education very seriously. Carter and School Resource Officer Bob Couchman began teaching Internet and technology safety courses to community members, students and other law enforcement officers about seven years ago. In these classes, Carter and Couchman walk participants through how information posted on social networking sites such as Facebook and MySpace can be used as pieces in a puzzle to compound a full picture that they never intended to share. They emphasize that when individuals share on these sites, they are not sharing with a select few friends and family, they are sharing with the world.

"That's what people don't think about because it seems so harmless — it is information that I would share in this room," Carter said. "But when you share, you are sharing with the world — that is good people, that's bad people. That's people you want to share with and those that come to you because they have something to gain from you and are hoping you have something to lose."

In student classes, Couchman will pull a random name off the class list and do simple Internet searches on the student to see how much personal information he can uncover just from the information that student has chosen to put on social-networking sites. Many times he is able to uncover information about the student's boyfriend or girlfriend, the student's parents' names and address and can bring up an image of the student's home on Google satellite. The wide-eyed looks he gets at that point often grab the students' attention and help them understand the importance of being guarded about how much information they make available, Couchman said.

"Social networking is a good thing if it is used correctly, but the thing we say time and time again is more is not better," Carter said. "A little chocolate tastes good; a whole lot of chocolate is going to give you cramps. That is the situation we are seeing.

"Many times our young people are led astray because of their lack of knowledge about social networking," he continued. "They put themselves in a grown-up world with the mindset of a child."

Often the best chance at reaching students and adults alike is having a connection with them, building a relationship or forming a friendship with them — allowing them to develop trust in the officer, Carter said.

"Everything we are discussing about social networking is not possible, cannot exist and will not be successful unless you have the trust of the individuals that you serve," Carter said. "Without trust, you are dead in the water.

"When an individual finds themselves dealing with social networking gone foul, their level of trust is gone," he added. "They are saying how did this happen? I don't understand — why me?"

Madisonville Chief Wade Williams is steering the agency toward a greater understanding of the importance of community partnerships and overall relationship building.

"The fact that they know a police officer and can pick up a phone and call — they've got to have a person they know as officer so and so, not just the police, but someone they know by name," he said. "With social networking and electronic information it is here to stay. It's either you choose to get in front of it and use it to your benefit or you get used by it.

"We choose to get in front of it and use it for the benefit of law enforcement and the community," he continued. "We want to get out there and make that partnership. When you build relationships in neighborhoods, they tie into you and trust you, and you can get more information and a lot more done because policing is something that a police department cannot do alone."

Relationships are vital because often what people put out through social-networking sites or via text and multi-media messaging they do assuming personal security. They are often in the comfort of their own homes and assume that the messages they type or the pictures they send are only going to the intended party. They believe that by being in their own >>

☐ Madisonville Sgt. Robert Carter (left) explains the intricacies of social-networking sites and the vast information that can be gathered from them, during a class he and Officer Bob Couchman taught to North-Hopkins High School freshman.



PHOTO BY ELIZABETH THOMAS

☐ Madisonville SRO Bob Couchman drives home some of the personal dangers involved in putting too much information on social-networking sites. Couchman, along with Sgt. Robert Carter (far left), have been teaching Internet safety classes in Madisonville and across the state for nearly seven years.



PHOTO BY ELIZABETH THOMAS

## LEN contacts for social networking sites

Madisonville Police Sgt. Robert Carter and Officer Bob Couchman encourage law enforcement officers to make the effort to find the law enforcement contacts with each of the popular social-networking sites. Each site has law enforcement contacts that can be so, so helpful, Carter said.

These contacts will make officers verify they are law enforcement, but Madisonville police have had good results with using these contacts in the case that something needs to be removed to protect a citizen.

Carter emphasized that it is important to establish those relationships in times of rest or peace because the times that officers find storms in life is not the time to go looking for this information.

Carter and Couchman have found that the law enforcement divisions within these social-networking sites are usually made up of retired officers.

"We've had things removed off Facebook within 30 minutes, boom, like it never happened," Couchman said.

Carter urges the law enforcement community to prepare now.

"My advice would be go ahead and make those contacts because at the end of the day it's better to have it and not need it, than to need the knowledge and not have it," he said.

For a jump start on finding the law enforcement contacts for sites such as Facebook, MySpace and Twitter, visit [www.search.org/programs/hightech/isp](http://www.search.org/programs/hightech/isp).



PHOTO BY ELIZABETH THOMAS

>> home, no one else is going to see them and it is therefore OK.

"Then boom, it just goes everywhere," Carter said. "Once it's posted, it's out there. We have to get that point into these kids' heads; they don't understand. What is cute to mom and dad, what is cute to my peers, what is cute tonight at this slumber party is indeed cute and funny to someone else that has ill intentions."

It all goes back to educating people about the implications of the choices they make, regardless of what type of privacy they think they have in the material they are obtaining or sending.

"There is something about the safety of being behind a screen," Carter said. "I can talk to you in written text and say things that I would never say to you verbally. The parameters of what we know to be normal and what we know as limits — sometimes in those times when each of us may not be thinking to the best of our abilities, things happen. Those things are irreversible."

This is not an issue that simply revolves around the home computer anymore. As more and more people are using iPhones and other smart phones that offer 24/7 access to pictures, video, texting and other social media, these issues have gotten even more difficult to combat. The immediate and constant access to mobile communication means that the information out there is not stagnate, it is constantly changing, every day, every second, Carter said.

"In regards to technology and social networking, we cannot risk being reactive," he said. "We have to take a

proactive approach to see what is going to be the best method and best vehicle to get individuals prepared to deal with this age of technology."

Three questions Carter suggested everyone should ask themselves before putting information out on social networks or sending messages through mobile phones are:

- Is this something I am comfortable sharing with the entire world — not excluding anyone, that includes my exes, the sickos, everyone — yes or no?
- Is this something I want to see 20 years from now or see posted on a billboard? It's cute now in high school, but one day I'm going to be a professional. And as a professional is this something that can come back and haunt me? Now it's not the photo album that sits under mom's coffee table that she embarrasses you with when you come home for family visits. It's out there.
- Is this something that you would be comfortable with your pastor or person you think so highly of seeing? Would you show it to grandma?

Giving people a sense of personal accountability is important in helping people not get used by the technology that they find so useful.

"There is no expectation of privacy on social-networking sites," Carter said.

But someone also has to take responsibility for reining in these issues before it becomes too big to handle, Carter stressed.

"No one has grabbed the reins and said 'Let's go' — it has to be law enforcement, we are the ones that have to do that," he said. "The responsibility is on us and since that is on us, we have to be prepared to deal with that from our citizens to our own families. As we build this ark it is going to take us all pitching in."

"Times have changed," he continued, "with change comes growth, with growth comes new responsibilities. With those new responsibilities we have the opportunity to see and experience a positive change. But seeing and experiencing positive change and growth also comes with growing pains — sometimes it is uncomfortable and that's where we are now."

Abbie Darst can be reached at [abbie.darst@ky.gov](mailto:abbie.darst@ky.gov) or (859) 622-6453.

# Legal Hacking: Finding What You Need For Your Case Online

KELLY FOREMAN | PUBLIC INFORMATION OFFICER



On Facebook's home Web page, creator Mark Zuckerberg touts that the site is, "giving people the power to share and make the world more open and connected."

He isn't kidding.

It's no secret that Facebook, which caters to more than 500 million active users, has its privacy flaws. But for law enforcement looking to exploit those flaws in an effort to catch dumb criminals, that's not necessarily a bad thing.

Kirby Plessas, an open source intelligence expert based in Washington D.C.

recently shared some of her skills with local law enforcement at the Department of Criminal Justice Training. Among the tricks of the trade she shared were tips on tracking criminals on Facebook, even when they think their pages are locked from anyone they haven't befriended.

"Facebook is holier than Swiss cheese," Plessas said. "People think they have their pages locked. They are not locked."

Although Facebook has worked hard to make its users think they're keeping their information more private, each time the Web mogul asks users to accept new

privacy settings, those who accept the default settings are actually dialing down their privacy, Plessas said.

And now, thanks to a simple online tool, those who haven't fully adjusted their settings for friends' eyes only are leaving quite a bit for law enforcement to track.

### ZESTY

Plessas identified several avenues for searching social networks, including one called Zesty. When you type [zesty.ca/facebook/](http://zesty.ca/facebook/) into your Web browser, the resulting plain, white page is unassuming. The page, owned by a Google engineer who wanted to expose Facebook's flaws, displays a simple search bar and a little encouragement: "What does Facebook publish about you and your friends?"

Here's how you can use it:

If you already know how to find your suspect's Facebook page, open a separate window on your computer and go to that page. When you have it open, look at the Web address (or URL.) At the end, there should be a number, or sometimes, a name.

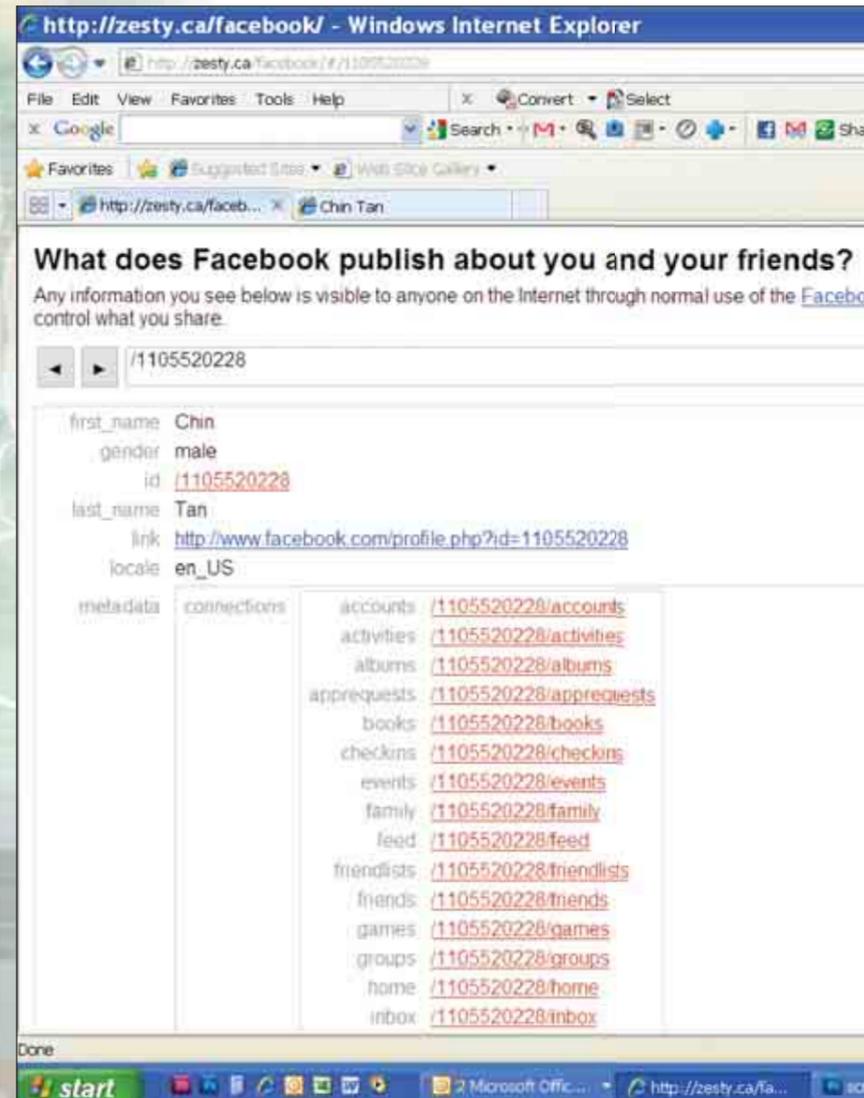
For example, it should look like this: <http://www.facebook.com/home.php#!/pages/KY-Dept-of-Criminal-Justice-Training/192289516870>

With your mouse, highlight and copy the number (192289516870, in this case) and return to the Zesty page. Paste or type that number into the search bar and click "Go." What appears seems convoluted, but look closely. There is a table with a label to the left that says "metadata." (See screen grab on the left.) Across from it you should see several red links that say things such as photos, statuses and videos. Clicking on those links will show you anything the user has left public.

"If it is really and truly not locked down, you can get in there and look at their photos, see their wall posts — I thought that was very helpful," said Eric Long, a Richmond police detective specializing in child and Internet crimes, who attended the class.

You can look at the photos and videos to identify your suspect as the right person, to see if they posted snapshots of evidence or victims, to see who their friends are to bring them in for questioning or any other reason you may discover to be helpful. Through the statuses, you can find

When searching for a suspect using Zesty, clicking the red links will take you to what they have available for the public online. You can read a person's status updates as well as how their friends respond, view their photos and more.



## Operators

Operators are key words that can be entered into search engines to search more specifically. For example, if you were investigating a case involving Mike Smith, a MS-13 gang member in Lexington, the following are some ways you could find results with the information about him and his online activity.

**Mike Smith Latin Kings OR Mike Smith MS-13** – find results with either Mike Smith and Latin Kings or Mike Smith and MS-13. Helpful if you don't know which gang he is associated with

**(MS-13) Lexington Ky.** – limits the results to information about MS-13 in Lexington, Ky.  
**"MS-13 Lexington"** – find the words inside the quotation marks next to each other in results

**MS-13 – Lexington** – find these words within 20 words of each other

**Inurl:MS-13** – every Web site that is returned will have these words within the URL (Internet address)

**Allinurl:MS-13 Lexington** – every word following the colon has to be in the URL

**Intitle:MS-13 Lexington** – only the word after the colon will be in the title

**Allintitle:MS-13 Lexington** – very specific, will find only Web site titles with MS-13 and/or Lexington

**(intitle:MS-13 OR intitle:Mike Smith) Lexington, Ky.** – will find sites with the two tied together in Lexington

**Site:gov MS-13** – Searches just web sites that have .gov at the end. The same works for .edu

**(Site:gov OR site:us) intitle:MS-13** – find sites with specific authority on the subject outside the parenthesis

**Site:FBI.gov intitle:MS-13** – reveals everything the Federal bureau of investigation's Web site has available online with MS-13 in the title.

**Site:FBI.gov** – searches only that site

**Filetype:pdf** – reveals PDF only results. Works the same with ppt abbreviation for power point results, mp3 for music files, or xls for Microsoft Excel documents

**Filetype:pdf intitle:methamphetamine site:gov** – reveals any PDFs about meth available on government Web sites

**Mike Smith Inanchor:MS-13** – reveals results with MS-13 in the links part of the Web address with the words Mike Smith on the page somewhere

Using these operators is commonly known as Google hacking. While the name sounds unscrupulous, it is perfectly legal.

"All you're doing is finding stuff on Google that is not as easily found," said Kirby Plessas, president and CEO of the Plessas Experts Network.

For more training materials, type `filetype:ppt intitle:google-hacking` into your search engine. □

**Kirby Plessas** is an Open Source Intelligence Expert providing training in Internet research techniques and analysis to a variety of law enforcement and intelligence agencies throughout the United States. An Army veteran trained as an Arabic linguist, she also worked at the Defense Intelligence Agency for Radiance Technologies in Military Geography and Urban Analysis. She has been declared the Department of Homeland Security Technical Expert for Internet Research. She consults and speaks to government entities about using Open Source and Social Media (Web 2.0) for their unique needs. Kirby has taught a number of classes for the U.S. Department of Justice. □

You can reach Kirby Plessas at (202) 684-8101 or [kirby@plessas.net](mailto:kirby@plessas.net).

>> out not only what they're talking about, but who is responding and what they have to say. Additionally, the friends responding on your suspect's page come complete with their own link to their pages, so you can feel out what public information they have to offer online, too.

If you don't know how to get to your suspect's page, to the right of the "Go" button, there is another search box. Enter in your suspect's name, email address or keyword and find them there. However, Plessas said this tool works best with the Facebook ID number.

*(Editor's note: It should be noted that using the standard "back" button on your browser will not work on this site. To go back*

*(or forward) to what you previously were viewing, use the arrows to the far left of the initial search box.)*

"When everybody had MySpace.com, you could get on there and look at all their photographs, see all their friends and everything they do," Long said. "But everybody has kind of switched over to Facebook and they have stopped that. You can see their picture if you can find them. So, I think this is of huge importance, to get in and see what they're doing. I have worked several cases of men supposedly talking online to juveniles and you get on their Facebook page or their MySpace page and you can see pictures of them with the victim. Pictures of them hanging out with

the victim. The same pictures on their MySpace site are on the victim's computer or vice versa."

Plessas identified another Web site, youropenbook.org, also seeks to showcase Facebook's not-so-private settings. A tagline on the main page reads, "Facebook helps you connect and share with the people in your life. Whether you want to or not."

The site searches public status updates of users with any keyword. Even without a Facebook account, an officer could type in something they are looking for by keyword — such as an assault rifle stolen at a recent home invasion — and see who might be talking about it. The site also brings up

users' photos and names along with anything they wrote.

"Facebook's bait-and-switch on privacy and their overly complex settings cause many users to post messages intended for their friends to 'everybody,'" according to the site's operators. "That's the entire planet, for all time. This privacy-malfunction could have serious consequences if you're looking for a job, applying for college or trying to get medical insurance."

Or, as Plessas said, if you're committing criminal activity and posting about it online.

#### TRACKING THEM DOWN

If you can't find what you're looking for from Zesty or Your Open Book, there still are other sites that make finding information much easier.

By going to [www.labnol.org/image-search](http://www.labnol.org/image-search), you can type in keywords and find photos people have posted on Flickr, MySpace or Facebook. If you are trying to match a username with a real name, Plessas recommends Web sites like [www.usernamez.com](http://www.usernamez.com) or [www.usernamecheck.com](http://www.usernamecheck.com).

Perhaps one of the more comprehensive search engines for finding all the ways people are connected online is through the site, [www.pipl.com](http://www.pipl.com). Pipl is a meta-search engine, which means it sends requests to multiple search engines and databases then combines the results into one, tidy list.

The site allows users to search using a person's name, email address, username or phone number. Results are pulled from everything from public records to blog posts.

"I probably use that one the most," Long said of [pipl.com](http://pipl.com). "I go to it before I go to Google sometimes because Google has so much information. [Pipl.com] shows multiple social networking sites. Like, if they had two and took their info off and now just have one, it will show all that."

But, these online tracking methods aren't limited just to the large-scale public profile pages. The micro-blogging giant, Twitter, has multiple back doors itself for law enforcement to find what they're looking for online.

Twitter, the 140-characters or less service known for quick information sharing, has even less privacy than its other social networking counterparts.

No one has to add you as a friend to see what they are saying.

"It's like the rumor mill on steroids," Plessas said.

But if you're looking to quick search information posted to Twitter, there are sites for that, too. [Search.twitter.com](http://Search.twitter.com) allows officers to search via keyword. But it also allows you to search all the tweets in an area with keywords called operators. For example, if you wanted to see everything Twitter users in Corbin were tweeting about, you would type "near: Corbin, Kentucky" into the search bar and it will generate your results for that area. As more tweets come into the site, the search engine also will continue to generate them as long as you have the page open. Simply refresh the page to see the new results.

There are dozens of other sites to search and monitor twitter posts, as well as the photos and videos uploaded by Twitter users. Some, like [searchtastic.com](http://searchtastic.com), allow you to export results to a Microsoft Excel spreadsheet. Additionally, Twitter and Google made an agreement in Feb. 2010 to make tweets searchable through Google, Plessas said.

#### RSS FEEDS

But, if visiting a handful of Web sites and sifting through search results sounds like time-consuming work, there's a simple answer. Literally. Real Simple Syndication, otherwise known as RSS feeds, is a way to bring everything you're looking for to you, as soon as it is updated.

News stories, blog entries, Tweets — even Craigslist postings — all can be delivered straight to you from RSS feeds delivered into an RSS Reader, such as Google Reader. So, if an officer was investigating a burglary case in which an Xbox 360 was stolen, an RSS feed could be established to send the officer news stories published online about the burglary; any comments made online about the case, people involved or the missing property as well as anytime a used Xbox 360 is posted on Craigslist for sale.

Creating a reader account is simple, too. It requires creating a Gmail e-mail address through Google and clicking on their "Reader" link. Many Web sites that have constantly updated information have a little orange button with a white graphic

that looks somewhat like pulsing waves. Clicking on this icon usually will take you straight to a link to hook that page into your reader. But even if the button isn't there to automatically link you to the information, it isn't hard to create the link yourself.

For example, if you wanted to create an RSS feed every time a used Xbox 360 popped up for sale in the Lexington, Ky. Craigslist group, here's how you would do it.

On your computer, go to [www.google.com](http://www.google.com). Then, in the search bar, enter [site:Lexington.craigslist.org](http://site:Lexington.craigslist.org) Xbox 360. Once Google has completed its search, copy the whole URL from the top of the search results page. In a new browser window, open the Web site [www.Bing.com](http://www.Bing.com). Paste the URL you copied into the search bar. Click search. Once the search results have populated, return to the URL at the top of the page and go to the end of it. Once there, type (without quotations) "&format=RSS" to the end of the URL and press enter. The results will bring you to a page with an option to add the feed to your Google reader.

Long uses RSS feeds to keep up with the news, but said it also can be helpful for gathering case information via Web sites like [Topix.com](http://Topix.com).

"People pass that off as a bunch of idiots sitting around gossiping," Long said. "But if you read on there, some of those people have first-hand information that nobody else would know unless they are directly involved. A lot of the cases that we work, they'll have information we haven't released yet. They sit there and talk back and forth to each other about it. It can be very beneficial." J

Kelly Foreman can be reached at [kelly.foreman@ky.gov](mailto:kelly.foreman@ky.gov) or (859) 622-8552.

□ If a person has selected Facebook's recommended privacy settings, you should be able to read the statuses they post as well as any comments on that status from their friends. Following the red links below their friends' names will take you to their pages, too, to view what information they may have left open for public view.

http://zesty.ca/facebook/#/1105520228/statuses

Control what you share.

/1105520228/statuses

data	comments	data	created_time	2010-04-11T03:14:02+0000
		from	id /573827683	
			name Matthew Walton	
			id /118139638196775_369696	
		message	Great one Coach! Do you like to sing your TN Vols song right after you tell that joke.	
			created_time	2010-04-11T05:13:41+0000
		from	id /606438807	
			name Casey Hutchens	
			id /118139638196775_370249	
		message	Did you hear the reason the Vols didn't make the Final Four...unfortunately they didn't have enough able to get out of their meetings with their probation officers. Don't worry though, our boys will send	
		from	id /1105520228	
			name Chin Tan	
			id /118139638196775	
		message	Did you all hear that Wall, Demarcus, Bledsoe, and Patterson went to play golf and did really well the first 14 holes, but they did the FINAL FOUR. So sad.....	
		updated_time	2010-04-11T03:09:57+0000	
	comments	data	created_time	2010-02-02T16:25:34+0000
		from	id /573827683	
			name Matthew Walton	
			id /282469738196_10657235	

# Social Networking and Law Enforcement:

## The Good and the Bad Are All Very Public

KELLEY L. CALK | STAFF ATTORNEY,  
DOCJT LEGAL TRAINING SECTION

Facebook. MySpace. Twitter. Digg. LinkedIn. Police Pulse. YouTube. These terms are familiar for those who are technologically savvy and challenged alike. Some people swear they will never join a social-networking site, but as such sites become more common, the people joining range in age from 13 to 100. They come from every race, religion and culture, with as many varied sites as there are users. A member can talk to someone in Italy as easily as he or she can talk to someone across town. But as great strides continue to be made in the technology available for personal and business use, careful consideration must be given as to how those tools can and should be used.

Statistics indicate that 47 percent of adults who are connected to the Internet use social-networking sites, for both personal and business use. Seventy-three percent of teens and young adults are members of at least one social-networking site. Facebook is the No. 1 social-networking site and has approximately 500 million users, with its members using the site an average of five and a half hours per month. Twitter processes approximately 40 million tweets a day from its members. And technology does not require that someone be connected to a computer in order to use the sites. With the wide variety of smart phones currently flooding the market, there are millions of mobile users on social-networking sites.

But what do all these statistics mean for the user — in this case, law enforcement officers? Like anything, there can be good and bad things about the use of social-networking sites. But make no mistake; it is all very public, no matter what efforts are made to keep it private. Keeping this important fact in mind, law enforcement officers can make the most of the benefits of social networking while avoiding its pitfalls and the liability issues that accompany those pitfalls.

### THE GOOD

Many police agencies around the nation, and in other countries, are setting up their own Facebook pages, available to the public to become “fans” of the page. Frankfort, Nicholasville, Taylor Mill and Greenville are just a few of the city police departments that have their own

Facebook pages. The Kentucky State Police also has its own Facebook page.

These sites keep citizens updated with what is going on in each respective jurisdiction. Agencies post press releases, traffic information, road work and department-sponsored community events among other things. It helps to foster better communication between the departments and their communities. Not only can it provide the departments an opportunity to show what they are doing in the field of law enforcement, it allows the citizens to provide constructive feedback on the department’s work.

In Canada, the Vancouver Police Department uses Facebook and YouTube in its recruitment efforts. Because today’s young adults are technologically savvy, the department is making an effort to meet them in a manner they use every day.

Young adults today do not always read the newspaper or more traditional news resources like older generations’. They do, however, use Web-based social-networking sites on a regular basis, sometimes two to three times per day. In order to connect and effectively communicate with this younger group of possible recruit candidates, the Vancouver Police Department keeps its Facebook page updated with the requirements to become a police officer as well as features about its officers. On YouTube, “The Promise” is a three-minute video that demonstrates various police tactics, set to a dramatic musical score. There are other videos on using canines, firearms training and SWAT.

The most important benefit of social-networking sites is the manner in which they can be used to help solve crimes, enable officers to locate suspects and make arrests and help in missing person cases.

In Maine, the Auburn Police Department was able to place on its department Facebook page, photos of three individuals from hotel video surveillance where hotel property had been vandalized. Visitors to the page identified the individuals and were able to provide anonymous tips as to the identities of the suspects. Arrests were made for burglary and criminal mischief. In another case, the police department was able to make an arrest of a juvenile

who had threatened his school with destruction on his Facebook page. The juvenile meant the comment as a joke but the threat was taken seriously by police.

Twitter and Facebook can help mobilize thousands of people in a missing person’s case. Family members of a missing person will often set up a page on a social-networking site and from that, the possibilities of what can occur are just about limitless. In the case of Chelsea King, a California teenager who had been reported missing after failing to return from a run, more than 6,000 volunteers came together to search for her after her parents created a Facebook page and its postings went out via Twitter. While the search ended in a tragic way, the police were able to find her killer quickly, using and cataloging information much more efficiently with access to the Facebook page created by Chelsea’s parents.

### THE BAD

“Working tonight looks like it’s going to be a rainy, boring shift.” “Watching a drunk guy take a water hose into his man pants ... not my idea of a good time.” “I HATE PEOPLE.” “Big drug bust — pics later.” These are a few postings out there on law enforcement officers’ social-networking pages. These are somewhat generic postings but have the potential to cause big problems for the officers down the road for different reasons. The same thing goes for these groups that law enforcement officers have been members of: “Make-it-Rain Foundation for Underprivileged Hoes.” “He-Man Woman Hater’s Club.” “Passed Out in Trashcans.”

From a hiring standpoint, a social-networking page can be a nightmare for the person hoping to be hired by a law enforcement agency. Seventy percent of U.S. hiring managers have rejected applicants based on what they have observed on an applicant’s social-networking page. It is not just what the applicant has posted on the page but who his or her friends are and what they have posted on the applicant’s page. And, it does not stop there. If a friend posts something unfavorable on their own personal page and links the applicant to that post, a potential employer will find it.

Racist or derogatory comments, likewise, can be the death knell for an

applicant. In social networking, the rule is often “a friend of a friend is a friend.” But in reality, that is not a good rule to follow. An applicant may not even get in the door to take the police test, based on the content of his social-networking page. The New York Police Department reviews social networking pages in the presence of potential recruits to weed out undesirable candidates.

A Lexington case makes officers in Kentucky cringe. A former Lexington police officer made an arrest of a well-known musician after a routine traffic stop. The case became anything but routine when complaints began to come in about the content of the officer’s MySpace page. A friend had posted a picture edited with the officer’s face, showing him standing with the celebrity he had just arrested. Further, the officer’s page contained derogatory comments about the citizens of his community, developmentally-delayed individuals and homosexuals. He eventually lost his job with the Lexington Division of Police.

There are more examples of officers across the country using poor judgment in their postings, such as posting pictures pretending to shoot someone; of a wrecked cruiser and then commenting “oops, shouldn’t have had that last beer;” of providing too much information about their thoughts on law enforcement, the people they arrest and the people they protect. All of it can, and will, have a negative impact on that law enforcement officer.

There are plenty of law enforcement officers who have social-networking pages who do not make those remarks, post inappropriate comments or “statuses,” or post inappropriate pictures. They are cognizant of choosing to accept people as friends and they actually know the people on their friends list. These officers love working in law enforcement and only want to do that job to the best of their ability. Social-networking sites can still get them into trouble.

Trouble will come in the form of loss of respect and credibility with the prosecutor and the courts. It will bring unwanted attention from defense attorneys. These officers post about the big drug bust their agency just had and post pictures standing next to the >>

# LEGAL SHORTS

>> evidence. And it IS evidence. These pictures on the social-networking page become part of the case. It can raise questions about the officer's credibility, his bias and his integrity. The defense attorney will find those pictures or comments about the case. A defense attorney will find the comment that the officer "arrested 4 scumbags tonight."

Another concern with social-networking sites is when officers are using the sites. Everyone knows that work computers are for work and should not be used for personal business. Many agencies provide in-car computers to their officers and almost everything on those computers is subject to an open-records request. Even if an officer is not using his work computer to post to a particular social-networking site, many cellular telephones, Smartphone and iPhones provide Internet access to these sites. While the argument can be made that the officer was not using provided equipment to be on the Web site, he or she is using agency time to be there. That time can be used doing work-related tasks rather than personal tasks.

### THE VERY PUBLIC

Nothing on the Internet can be 100 percent private. Depending on the individual's skill in searching, anything can be found. Even when all privacy settings are enacted, there is no guarantee that something you put on someone else's page will be seen only by that person. Items found on social-networking sites posted by you or about you can be used against you in court to attack your credibility or impeach your testimony. Those working in the law enforcement field must find a balance between their personal and professional lives. It seems that if officers just used common sense, there would not be any issues when using social-networking sites. But common sense does not mean the same thing to every person, so these general guidelines are a good start to finding that balance between being a private person and being a law enforcement officer.

### IF YOU DON'T WANT EVERYONE TO KNOW IT, DON'T POST IT.

Some things are just better left untyped.

### DO NOT POST FROM WORK COMPUTERS OR DURING WORK HOURS.

Social-networking sites are just that — social. The purpose is to be able to connect with friends, family and even colleagues to socialize. And the time for that is when you are not on the clock. Misuse of electronic media can more likely than not lead to discipline action being taken against you.

### IF YOU WOULD NOT WANT YOUR GRANDMOTHER OR BOSS TO READ IT OR SEE IT, THEN IT IS PROBABLY SOMETHING THAT SHOULD NOT BE ON YOUR PAGE.

This is old-fashioned but effective.

### DO NOT POST IDENTIFYING INFORMATION ABOUT YOUR AGENCY SUCH AS THE NAME, LOGO, VEHICLE, BADGE OR OTHER TYPES OF SYMBOLS.

If this rule is followed, a lot of issues can be avoided. Many officers like to post a picture of their cruiser but should not. Take it down if it is on the page but know that just because it has been removed does not mean that it cannot be found. At least if an issue arises, you will be able to say it is no longer there.

### DO NOT POST ANYTHING (PICTURES OR STATEMENTS) ABOUT ANY CASE IN WHICH YOU ARE ACTIVELY INVOLVED.

Prosecutors and defense attorneys will be out there doing a Google search on you to see what is out there. That includes statements made about thugs, low-lives and people who deserve a beat down, as well as information related to specific cases.

### BE AWARE OF THE PRIVACY SETTINGS OF ALL SOCIAL-NETWORKING SITES TO WHICH YOU BELONG AND USE THEM.

This is not a fool-proof method but it will go a long way in keeping your information more private.

### KNOW WHO YOUR "FRIENDS" ARE AND WATCH WHO YOU "FOLLOW."

For law enforcement officers in particular, a "friend of a friend of a friend" is not a friend of yours. Guilt by association really matters here. You exploit that motto in your job as an officer, do not let it be used against you.

While only a select number of issues facing law enforcement officers when using social-networking sites have been discussed here, the original intent for the sites is to be an excellent tool for connecting with family, friends and colleagues. Sites can be used for professional purposes as well as personal. Because law enforcement officers are the trusted protectors of their communities, the good is really good and the bad can be really, really bad. And, it is all very public — accessible by anyone, anywhere. Keep that in mind as we all move into the future of continued technological advances. Good judgment and professionalism will enable law enforcement officers to benefit from social networking while avoiding its pitfalls. J



## No Texting Law Now in Effect

"No Texting" is now in effect.

Although the ban on sending or reading text messages on a personal communications device took effect in July 2010, until January 1, 2011, officers were only permitted to give warnings for violations. Because of the delay, many officers did not receive the violation codes for these offenses, as they were not included with the July update that covered all the other new laws that took effect at the normal time. Both offenses are violations.

### The codes are as follows:

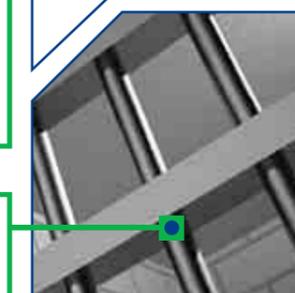
- 00266 – 189.292 – Communication device violation, 1st offense.
- 00267 – 189.292 – Communication device violation, 2nd or subsequent offense.
- 00268 – 189.294 – Communication device violation, < 18 YOA, 1st offense.
- 00269 – 189.294 – Communication device violation, < 18 YOA, 2nd or subsequent offense.

## Military Leave Reminder

With so many law enforcement and telecommunications personnel serving in the military, it should be noted that in 2006, the Kentucky General Assembly made a change in the number of days of annual leave such members must be given. KRS 61.394 and .396 provide that all state and local employees shall be paid their regular compensation for up to 21 calendar days per year, when in the performance of duty or training in their respective branch of the military (or the U.S. Public Health Service). Unused leave may be carried over for up to two years.

## Questioning Suspects in Custody

When a suspect is already in jail, having been arrested on a warrant, may an officer go to the jail to question the suspect? In such situations, timing is critical. Of course, the subject must be advised of *Miranda* rights, but if the right to counsel already has attached, either because they have specifically invoked the right, or because counsel has been assigned at arraignment, the subject must specifically waive the right to have counsel present. If an attorney has already made an appearance in the case, it may be advisable to contact the attorney, if the subject is willing to talk.



## New Definition of Family Member for Domestic Violence

The definitions of "family member" for the purposes of fourth-degree assault changed with the passage of 2010 House Bill 1, also known as Amanda's Law. This change went into effect on July 15, 2010. The legislature removed language defining the phrases from KRS 431.005(2), substituting instead, a reference that matches the meaning to the same terms in KRS 403.720. This removed the often-confusing phrase – "related by consanguinity [blood] or by affinity [marriage] within the second degree." The new definition of "family member" is as follows: spouse, including a former spouse, a grandparent, a parent, a child, a stepchild, or any other person living in the same household as a child if the child is the alleged victim.

As such, siblings, in-laws, first cousins and aunts/uncles are no longer automatically "family members." They will only be family members if they live in the same household as the perpetrator and they are younger than 18 (assuming they are the victims) or if (as the perpetrator), they live in the same house as the victim, who is younger than 18.

## Pregnancy and Drug Use

Last year, the Kentucky Supreme Court reinforced a previous ruling which states that a female cannot be charged with endangerment or abuse of her child based on having ingested illegal drugs while she was pregnant.

In 1992, the General Assembly passed the Maternal Health Act, 1992 Ky. Acts, ch. 442. The Preamble of that act strongly suggested that the General Assembly intended that maternal use of drugs or alcohol during pregnancy would not subject the woman to any additional punishment for the risk posed to the child in the womb. (In other words, she could be charged with possession, but not with wanton endangerment or assault where the child is the victim.) The purpose of this was to prevent women from being discouraged from seeking medical care because they feared prosecution for drug or alcohol abuse. The following year, the Kentucky Supreme Court interpreted that provision to dismiss the charge of criminal abuse against a mother who had used oxycodone during her pregnancy. See KRS 214.160(5)' Com. v. Welch, 864 S.W.2d 280 (Ky. 1993); Cochran v. Com., 315 S.W.3d 325 (Ky. 2010). J