How Social Media Is Changing Law Enforcement

Wayne Hanson | December 2, 2011

About This Report

This report is based on the activities of the Digital Communities program, a network of public- and private-sector IT professionals who are working to improve local governments' delivery of public service through the use of digital technology. The program — a partnership between Government Technology and e.Republic's Center for Digital Government — consists of task forces that meet online and in person to exchange information on important issues local government IT professionals face.

More than 1,000 government and industry members participate in Digital Communities task forces focused on digital infrastructure, law enforcement and big city/county leadership. The Digital Communities program also conducts the annual Digital Cities and Digital Counties surveys, which track technology trends and identify and promote best practices in local government.

Digital Communities quarterly reports appear in *Government Technology* magazine in March, June, September and December.

Introduction

There's a scene in the 1990 movie *Dances With Wolves* in which Kevin Costner's character Lt. Dunbar is traveling with a teamster by horse and wagon to his new post on the Western frontier. They come across a skeleton lying in the grass — an arrow sticking up through its ribs — and the teamster says, "Somebody back East is sayin' 'why don't he write?'"

Today, public safety is a bit more sophisticated, and methods of communication much faster. Law enforcement tools have evolved from wanted posters to police radio, patrol cars and social networks, such as Twitter, Facebook and YouTube.

Community policing today has also expanded through social networking to locate missing children, alert neighbors of suspicious activity and even inform the public about crimes committed in their neighborhoods.

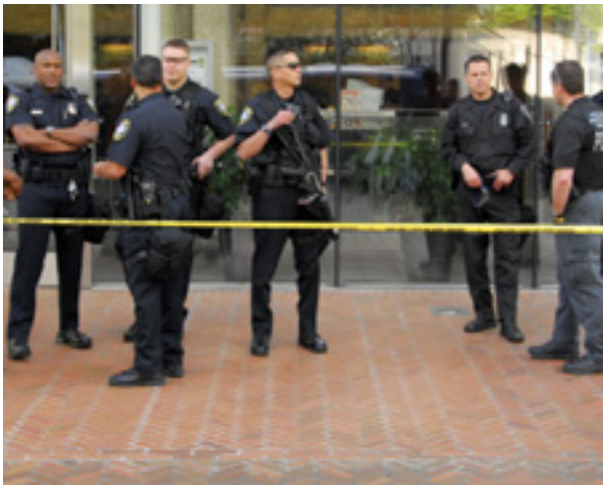
But social networking is a tool that cuts both ways. Flash mobs organized online in Philadelphia swarmed stores to shoplift and attack pedestrians; pedophiles use social networking platforms to share photos and video; and terrorists recruit members and plan attacks via these tools.

Even the courts have been affected. Jurors have disregarded instructions and have conducted online research, shared their opinions on Twitter from the jury box, and even posted biased comments on their Facebook pages.

In Albuquerque, N.M., a police officer discredited both himself and his department by listing his occupation on Facebook as "human waste disposal." And in a number of high-profile cases, officers have found their actions posted on YouTube and the subject of hundreds or even thousands of negative comments.

From a 140-character tweet to a 56 MB video clip, social networking is a force that cannot be denied or ignored. We hope this special section will assist law enforcement in embracing and understanding this phenomenon.

—



On the 10th anniversary of 9/11, Americans were reminded once again that law enforcement is engaged in an escalating war of new threats, weapons and technologies. It's a war in which perpetrators can recruit, organize and plan electronically beyond the reach of traditional policing methods. Communication is mobile, motivation may be mass destruction and targets include the innocent. As law enforcement agencies grapple with this new reality, they inevitably encounter social media and social networks.

In August, for example, Philadelphia Mayor Michael Nutter announced an expanded curfew for minors following flash mob violence. Flash mobs — organized online through various social media — convene at a predetermined time and place for a specific purpose. Though many are harmless or merely pranks, in Philadelphia, the purpose was to rob pedestrians and then swarm through stores shoplifting.

In San Francisco, following a shooting by transit police, protests were organized online in an attempt to block Bay Area Rapid Transit (BART) stations. In perhaps an ill-considered response, BART shut down wireless service in the subway to disrupt organizers, which outraged protesters and created yet more trouble.

But social media is having a positive impact, too. The platforms can be used by law enforcement to broaden intelligence gathering and leverage public support. "We had a very clear example of the importance of that this summer," said Sgt. Sean Whitcomb of the Seattle Police Department, "when a person became aware of a plot to kill soldiers and civilians at a military processing center with automatic weapons and grenades."

The Fort-Hood-style plot involved several individuals who were planning a large-scale massacre, said Whitcomb. "Someone came forward and talked to one of our detectives.

We got a joint terrorism task force involved and worked with the feds. The two suspects were arrested, and no one was hurt."

Social networking rapidly has become a valuable intelligence-gathering tool for law enforcement agencies, as well as a source of evidence for defense and prosecution personnel who search Facebook pages, Twitter feeds or YouTube videos seeking to discredit witnesses, establish law enforcement bias, track down evidence or establish associations between gang members. Often, perpetrators brag about their crimes on social networks, and child pornographers and sexual predators have been located and apprehended as a result of their online activities.

Mistrials also have occurred because jurors have disregarded instructions and researched cases online, used Twitter to share their opinions from the jury box, or have posted biased comments on their Facebook pages. For example, in late 2010 during the Chandra Levy murder trial, a prospective juror was dismissed for using Twitter to discuss the case. And in another case, a juror in California was discovered blogging details of a murder case during the trial.

Although social media can help enlist public support, it also can turn on a dime and do the opposite, due in part to the casual nature of the media. In a wake-up call for law enforcement, an Albuquerque, N.M., police officer involved in an on-duty shooting brought discredit to himself and his department when reporters discovered that he listed his occupation as "human waste disposal" on a Facebook profile. And in several high-profile cases, officers' actions have been posted on YouTube, receiving hundreds or even thousands of negative comments.

Boston police tried to stop the public from videotaping officers under the state's wiretapping act, and arrested an attorney for recording officers with his cellphone. In that case — Glik v. Cunniffe — the 1st U.S. Circuit Court of Appeals ruled that such videotaping is a free speech right protected under the First Amendment. Mobile devices and social media bring football's instant replay capability to law enforcement and to thousands of armchair quarterbacks around the world. It's also important to remember that nothing on social media ever goes away.

Law enforcement agencies around the country may see social media as a double-edged sword, but it's here to stay and must be placed in the tool belts of officers and departments.

According to Dunwoody, Ga., Police Chief Billy Grogan, embracing social media is one of the smartest decisions law enforcement can make today. In an article written for the International Association of Chiefs of Police, Grogan outlined three reasons for this: Social networks offer a natural platform for extending community policing efforts. They provide a way for departments to promote positive accomplishments. And finally, the continuing popularity of these networks simply makes them hard to ignore.

"The need is there. The people are there," Grogan wrote. "Why aren't you and your department?"

Investigations: The Good

Lt. Charles L. Cohen of the Indiana State Police has been training state and local police agencies on social media usage since 2002. He said that while criminals are

using mobile devices to hide their activities, social media offers huge benefits to law enforcement.

Lt. Charles L. Cohen of the Indiana State Police has been training state and local police agencies on social media usage since 2002. He said that while criminals are using mobile devices to hide their activities, social media offers huge benefits to law enforcement.

For example, pertinent information can be learned if a member of a criminal organization attends a family reunion and then a video of it is uploaded to YouTube. "That helps investigators put faces with street names and put people in association with others, when you ordinarily wouldn't be able to do that," Cohen said. "Even five years ago, if you wanted to show an association between two people, you had to do surveillance. Now you can just go to blogs, video or image sharing sites, and in many cases, find those pictures."

Images on social media sites also often yield other information of interest to the investigator. Photo background information was used last year to find a child pornographer and his victim, Cohen said. Metadata and geotagging of images can help locate where and when photos were taken.

And it's not just social media that's providing easily available information. Investigators also can get help from government websites, which now provide large amounts of information online. " Most assessors' offices [and] most county recorders put information on the Internet about your house," Cohen said. "You can find out online where I bought my house, when, from whom and how much I paid for it. You can find out who my neighbors are, what my neighbors do for a living — all this information is available."

Whitcomb explained that checking social networks for information is now routine investigative work. "Let's say we get a name of a possible suspect in a shooting, would I look to see if that person had a Twitter or Facebook account? Of course I would. It's just detectives doing good detective work. You need a warrant to go where the public can't go. But if you can grab it online, you're good to go. It's like electronic canvassing — no different from going out door-to-door saying, 'Did you see or hear anything?'"

Mike Edwards, a special assignments lieutenant with the Seattle Police Department's Criminal Investigations Bureau, said criminals sometimes think they are anonymous online. "There was a prolific motorcycle thief," he said. "We found out he had a Facebook page, and he would post photos of himself on the stolen motorcycles. With that evidence, we were able to get a conviction. Some of them he took to chop shops, and we were able to arrest folks in the chop shops as well. So that was purely a social media tool."

Edwards, a 31-year police veteran, said some cases lean heavily on social networking. Another example included a blog post that had references to social media and chat rooms, which detectives determined were being used by a pimp. "We were able to secure the arrest and recover two juvenile prostitutes and reunite them with their families."

An investigation now, said Edwards, "covers the gamut, from your Craigslist-type postings where it's seller-to-seller with fraud going on, all the way to an individual

who is using social media to share specific criminal knowledge or evidence with other individuals because they're so darn proud of what they're doing."

Seattle police also use social media for early warnings about events that can impact public safety. For instance, city leaders monitored social networks on the proposed Sept. 17 "Day of Rage," which fortunately didn't amount to much.

"We want to make sure we've got enough staff to ensure that people who demonstrate can do so safely, that traffic can move, and that public safety is achieved," Whitcomb said. "So that's just proper planning."

Investigations: The Bad

But social networking tools are also increasingly used by criminals, and that can make police work more difficult. The example of Philadelphia's flash mob problem highlights how social media can be used against the public good.

Criminals using small mobile devices can create havoc, Edwards said. "Everything from sending out viruses and accessing protected sites, sending false IDs — all that can be done at the speed of fingertips, where in the past it took a lot more time and effort. And the footprint left behind is so much smaller now," he said. "In the past it was difficult to get rid of evidence, but it's extremely easy to get rid of it now, and a lot more difficult to go and uncover it, so our investigative speed has had to increase to match this. The resources that we've had to draw on have also expanded dramatically, because the number of sources is so many."

The biggest problem for local law enforcement has to do with obtaining and retaining social media records, said Indiana's Cohen. "I see this video of a gang fight or a guy holding a sawed-off shotgun. But how do I download the video so that I can take it into court a year from now, knowing it might go away the minute I refresh my browser?" Cohen said officers or investigators must be able to obtain the records and understand them well enough to establish that the video was uploaded from a house or mobile device owned by the suspect, for example.

Another problem is that even though a criminal may be using Twitter or Facebook in a police department's jurisdiction, the company operating the platform may be based in another city or even a different country. In the past, a police officer investigating a crime could go to the phone company's local office or the local bank branch to obtain records. "But if I'm using voice over IP to communicate, there may be no physical presence in a local jurisdiction, or even in the United States," Cohen said. "Skype for example, is incorporated in Luxembourg. And if somebody is communicating via Facebook, that means, as an Indiana police officer, I need to serve a search warrant on a California company — with no storefront or physical location where I can go."

Cohen said 80 to 90 percent of U.S. police agencies have fewer than 50 sworn officers, and securing records for a company outside the United States can involve the U.S. State Department, international treaty issues, embassies and other complexities that are very difficult for a small department to navigate.

The vast amount of information on the Internet, along with the organizing power of social media, also can make it easier for criminals to succeed.

“In the past, the knowledge of how to commit a crime — a burglary or how to crack a safe — you had some specialists and some other people who weren’t all that good at it,” Edwards said. Today, criminals can find instructions online — or even be prodded to join an event like a flash mob through a post on a social media platform. “The force multiplier of the number of people who could do these things is dramatic,” he said.

And finally, law enforcement personnel must beware of what they put on their own pages, said Kara Owens of the Minnesota Department of Public Safety (DPS). “I talk to the new troopers and tell them not to say where they work. ... If you typed ‘Minneapolis Police’ [into a social media site] and a bunch of police officers showed up with their pages and family photos with information on where they live and so forth, that would be a danger to the officer.” In addition, an officer who posts photos from a GPS-enabled smartphone can unknowingly reveal the location of his or her home or office to a criminal with the right software.

Informing the Public

In August, as Philadelphia officials were coping with flash mobs, the Digital Communities program traveled to that city for a meeting of its Law Enforcement Information Technology Task Force, which was held in conjunction with the Association of Public-Safety Communications Officials conference. Among the attendees was Seattle Chief Technology Officer Bill Schrier, a task force member, who showed off a new iPhone application that lets citizens track 911 calls in the city. But that, it turns out, is just the tip of the iceberg. Seattle’s use of social media provides a study of how innovation can be used for the benefit of law enforcement and community.

For instance, the city’s website includes an interactive map showing 911 incident responses, police reports and crime statistics.

“Fire 911 calls have been public since 2002, but the mapping of them happened about three years ago,” Schrier said, adding that the city delays posting police 911 calls for several hours to keep citizens from showing up during dangerous incidents.

“Fire 911 calls have been public since 2002, but the mapping of them happened about three years ago,” Schrier said, adding that the city delays posting police 911 calls for several hours to keep citizens from showing up during dangerous incidents.

Police reports posted to the site are redacted and usually appear 24 to 48 hours after an incident. “I think that’s unique, I don’t know if there are that many places in the United States that put redacted police reports online for anybody to see,” Schrier said.

Posting police reports online is, in part, a reaction to the changing nature of the news media. Up until a few years ago, city police dealt with a handful of newspapers and television and radio stations. Reporters would monitor radio dispatch activity — or police spokespeople would contact news outlets when a major incident occurred — and pick up paper copies of police reports at the station. But an explosion of neighborhood bloggers and other online media made providing paper reports a burden for city police.

In response, Seattle began burning reports onto DVDs, but that was a lot of trouble too. Putting reports online solved the problem. “ That way the media has it and anybody else who’s interested has it too,” said Schrier. “If you need an unredacted version — like if

you were in a car accident — then you could come downtown and get the unredacted version."

The online incident maps also support the city's 1,200 registered " block-watchers," who are small groups of people in neighborhoods who work together to keep themselves safe and monitor crime and other goings-on. The 911 mapping is a way to assist them and also encourage them to contribute data to law enforcement.

"They can have data from the last few days about what's going on in their neighborhood, and they can take appropriate action. So it puts more tools in the hands of citizens," Schrier said, adding that posting the information also reduces police workload. "Instead of calling 911 for suspicious activities, block-watchers would immediately know if it was suspicious or not because they've been sharing information online."

Behind Seattle's social media activities is a sophisticated records management system that serves a multitude of purposes.

"The fire 911 calls come directly from the computer-aided dispatch system for fire," Schrier said. "Typically a call will show up on the website in one to three minutes. So I tell people, 'You see a fire apparatus go by your house, go to the website, and chances are good that it will already be on the website.'"

That feature required technology. Schrier said the city spent about $250,000 for its information dissemination system, which feeds an internal Police Department database that's used from crime analysis. It also automatically creates redacted police report data that populates the public website and is used by various city departments. In addition, the system shares police data with the city's Law Department, which prosecutes cases, and the municipal court.

Community Policing

As Seattle's experience shows, social media can be an important component of community policing. That's also true in the relatively small town of Dunwoody, population 47,000, where Chief Grogan said social media is an enhancement to its efforts. "Community policing is manpower-intensive to some degree, because people have meetings and you have to send somebody to them," he said. "We still do those

sorts of things, but you can reach far more people through social media than you could ever reach by attending meetings.”

Seattle’s Whitcomb said that to be truly effective, community policing must go where the public goes. And these days that means social networks. The police department routinely distributes information about crimes under investigation — including pictures and license plate numbers — via social media.

“We make appeals regularly for witnesses to come forward through Twitter and our blog. So broadly, we do enlist social media to help solve cases,” Whitcomb said. “Years ago we would send out news releases, we’d hold press conferences — nowadays we can bypass all that. We just put it on our website, and then reach out on popular social media sites like Facebook and Twitter. We believe we’re hitting a bigger audience.”

Some community policing initiatives have been started by the citizens they serve. For instance, when software company owners Keli and Robert Wilson lost track of their children at a large California amusement park for 45 minutes, the experience spurred an idea.

“I realized I didn’t have an updated photo of them, so I couldn’t go up to security and say, ‘Here they are. Please go and look for them,’” said Keli Wilson. The Wilsons developed My Family, an online repository of information about children that contains a recent photo, their height and weight and other information. If a child is lost, law enforcement can get immediate online access to current information even if the family is far from home. From that evolved AlertID, a comprehensive public safety service that launched in Washoe County, Nev., in 2010.

“We were approached by Washoe County Sheriff Mike Haley,” Keli Wilson said. “So we’ve become a sort of neighborhood watch on steroids.”

According to Keli Wilson, residents of a participating jurisdiction sign up and provide an address. The AlertID application shows crimes that occur within a three-mile radius of their location as icons on a map. “They also get text and email alerts when something happens,” she said. “For example, if there’s a residential burglary or a sex offender moves into their neighborhood.

“Another part of it is a social networking component we call Community Watch, where the public can use social networking to communicate with one another — for example,

about a suspicious vehicle in their neighborhood, a solicitor or an attempted abduction. We also give law enforcement the ability to broadcast, for example, a missing elderly person, a school lockdown, a shooting, etc."

AlertID includes a mobile phone app, so that users can access data and receive alerts and other information when they're on the move or away from home.

Washoe County Commissioner Bonnie Weber said AlertID started as a pilot with about 700 people, and it's grown to about 15,000 people/residences subscribed in Washoe and Clark counties, as well as the cities of Henderson and North Las Vegas, with more in the planning stages.

"It's relatively easy to be able to get online," said Keli Wilson. " It's free to the public, it's free to law enforcement, and thus far we have been self-funding it. But we expect family friendly companies to sponsor areas."

Getting Connected

Social media helped the newly created Dunwoody Police Department build ties to the community shortly after the city incorporated in 2008. "We wanted to find a way to reach out," Grogan said, adding that there already were several community blogs in the area and many people online. "We started out from day one using Twitter, and then shortly thereafter we added Facebook and YouTube."

Social media also can help police departments distribute positive stories that may be ignored by mainstream news outlets. "We know that our staffs do an amazing job each and every day operating under difficult and stressful conditions. Yet little of what they do ever gets published," said Grogan in a recent article on the IACP website. "They make big arrests, they provide great customer service, they go the extra mile, they win an award, they save a life, and the list goes on and on. Social media can and should be used to educate the public about what your department does, how they do it and build confidence and trust in your agency."

Some departments, especially larger ones, shy away from using social media, fearing they'll be overwhelmed by citizen comments. But Minnesota's Owens said there are techniques to manage citizen interaction, and that the positives of social media will outweigh the negatives.

"It's a free way to get your message out," Owens said. "Think of it as your own news channel. If you have a story you need to get out there, get it out there."

She said the traditional media now monitor DPS social media and have picked up a number of the department's posts. "We use Twitter when there's a bad crash. For example, there was a big backup because of a rollover on Sunday. We tweeted a rollover on 35 just north of the Burnsville Split, no serious injuries but a big backup. In the winter when we have a big snowstorm, we tweet how many crashes and cars are off the road, that sort of thing."

Owens said the feedback has been rather positive. "People like that we are communicating with them, and we're telling our stories."

To reduce incoming traffic, the department only allows the public to comment on DPS posts. “So a random person wasn’t posting on our wall without us knowing,” Owens said. Comments appear as soon as they are posted, and Owens keeps track of what’s appearing. She utilizes a Facebook setting that emails her when someone comments on a post, picture, album or video.

Owens handles social media pages for the Minnesota State Patrol, DPS, Homeland Security and Emergency Management division, and Bureau of Criminal Apprehension. The State Fire Marshal’s office handles its own page.

The DPS also uses Facebook, Twitter and YouTube to publicize events like the department’s “Maroon Day” patrols. Maroon Days — named after the State Patrol colors of maroon and gold — are high-traffic days where every state trooper is on the road enforcing Minnesota laws. To prepare, said Owens, “We did a big social media push. I went on a ride-along with our lieutenant and produced a video on YouTube. And then on the actual Maroon Day, the State Patrol tweeted with hashtag #MSPmaroonday, how many people they had pulled over for things like seat-belt violations, [driving while intoxicated], etc., and how many crashes.”

The DPS also uses Facebook, Twitter and YouTube to publicize events like the department’s “Maroon Day” patrols. Maroon Days — named after the State Patrol colors of maroon and gold — are high-traffic days where every state trooper is on the road enforcing Minnesota laws. To prepare, said Owens, “We did a big social media push. I went on a ride-along with our lieutenant and produced a video on YouTube. And then on the actual Maroon Day, the State Patrol tweeted with hashtag #MSPmaroonday, how many people they had pulled over for things like seat-belt violations, [driving while intoxicated], etc., and how many crashes.”

The city also updated the traditional police ride-along for the social media age. A “tweet-along” — where members of the public spend time with officers and tweet in real time about their experiences — helps residents better understand what police officers are doing and how they protect the public.

Owens said agencies of all sizes need to have a presence on social media. “If Facebook was a country, it would have the third largest population,” she said. “But once you post something, it’s out there — even if you delete it. So think before you post. And you don’t have to be a grammarian — write like you talk.”

In addition to providing an outlet to communicate with the public, social media can help agencies interact with the news media. Owens said the department tweets when the lieutenant is available to comment on a crime or case, which streamlines the public information officer’s job.

The Old and the New

Embracing social media does not negate traditional police work. Ultimately cops still deal with human beings and law enforcement remains a one-to-one business. But social media is becoming an important tool for officers and public safety agencies.

“We’re always looking at technology and where we can best utilize it. We’re bringing people into the workforce as well who have that aptitude,” said Edwards. “We had Polaroids, then we had 35 mm film for decades. Now we’re moving through these different platforms far more quickly. Some of it is our own demand. We’re pushing vendors and engineers and the rest to get us these tools, because we see the utility and the benefit for them; in some cases, [we’re] even designing them ourselves.”

For instance, as more people migrate to mobile devices and tablets, it will be important for cities to have applications that run on those platforms, Schrier said. While Seattle’s immigrant communities have fewer home computers, most have mobile devices and smartphones, so applications and websites should be able to interact with people via those platforms.

As the use of social networks evolves, it’s vital for law enforcement agencies to watch their peers and share their experiences.

“We’re constantly looking at what other people are doing and how they’re doing it. There’s a lot of communication going on between agencies now, and the willingness to share has increased dramatically,” Edwards said. “We all realize that we may have come up with a really good idea, and the only way others can get it is if we share it with them. And if we tried stuff that didn’t work, we can help others avoid the same pitfalls.”

http://www.govtech.com/public-safety/How-Social-Media-Is-Changing-Law-Enforcement.html