Undercover Online

> BY CAREN CHESLER
> ILLUSTRATION BY ALEXANDER WELLS

SOCIAL NETWORKS ARE THE NEW FORUM FOR THE CAT-AND-MOUSE GAME BETWEEN POLICE AND CRIMINALS.

ABOUT THREE TIMES A week, Susan James, a 37-year old blond prosecutor from the Midwest, signs on to Facebook as Nakesha*, an attractive 26-year-old with a dark ponytail and sunglasses that conceal her eyes.

James created Nakesha's profile from a photo she found through Google. Her favorite TV shows? *Keeping Up With the Kardashians* and *For the Love of Ray J*. Her favorite quote? "What doesn't kill me makes me stronger." She even has a fake birthday, on which her Facebook friends sent her birthday greetings like, "Yo, happy birthday, mama."

When Nakesha is online, James is undercover. She structured the profile as bait for local criminals, whom she chats up to get a glimpse into their operations. Nakesha now counts drug dealers, gang members and their girlfriends among her 76 friends.

"Nakesha has more friends than I do on my own account," James says.

But both women are primarily interested in one man—a drug kingpin James has been investigating for several years. He's been arrested more than a dozen times but has never gone to jail—in part because he's careful. He changes cellphones, SIM cards and cars as often as most people change their socks.

James has actually used her Facebook presence to help wiretap a

**Names have been changed, as this is an active investigation.*

phone registered to one of the kingpin's associates. Drug dealers often register phones to bogus names like Mickey Mouse. But when James, through Facebook, asked the associate what his plans were one night, he responded through an app he had downloaded to his iPhone. Her office quickly tracked the purchase to identify the number.

Like almost every other aspect of modern life, street crime is now deeply intertwined with digital technology. And social networks in particular have become part of the organizing structure of criminal networks—from street gangs to political agitators.

To infiltrate these networks, law enforcement officials in both small police departments and large government agencies spend an increasing amount of time looking for criminals on social media websites such as Facebook, Myspace and Twitter. While they used to go undercover on the street, cops now gather intel online, mining suspects' profiles for photos, accomplices and potential evidence.

"Criminals leave footprints everywhere they go—on their cellphones, on their Twitter accounts and on Facebook," says Lauri Stevens, a principal strategist at LAwS Communications, a firm that consults with law enforcement on social media strategies. "With advances in geolocation technology, detectives don't just know what the criminal did, but where they did it. Social media can give them a solid and reliable way of piecing things together."

Many police departments first made the move online in child-predator investigations, in which a detective might pose as a child to snag a pedophile. But the techniques are now used in all areas of law enforcement.

"There was a time when if you handed a cop a laptop, he'd want to throw it out the window," says Boca Raton Police Chief Dan Alexander. Now, most officers won't part with their iPhones, he says.

Gang-Busting

SOCIAL MEDIA HAS PROVED IRRE-sistible to gang members, says Bruce Ferrell, president of the National Alliance of Gang Investigators' Associations. Gangs use the medium to coordinate crimes and recruit new members, but they also like to show off, posting photos of hand signs, colors, weapons, drugs and cars, all of which can identify an individual as a gang member.

These digital clues have led to numerous busts. Last year, federal authorities arrested six members of East Side Riva, a Riverside, Calif., street gang, after finding communications the group had sent over Myspace and rap videos it had posted on YouTube to intimidate enemies.

In 2008, a multiagency task force arrested a Miami gang leader known as Bird Road Rudy after he posted a YouTube video of himself and his friends waving guns in the air and taunting Miami police. The courts sentenced him to six and a half years in jail on federal weapons charges.

Why are gangbangers so eager to incriminate themselves? Mike Bostic, a retired Los Angeles Police Department assistant chief, chalks it up less to stupidity than to audacity. "The nature of gangs and criminals is that they can't wait to brag about what they're doing," he says. "They start posting on Twitter and Facebook, and all we have to do is sign up like everyone else and get into the system. Soon, we know what they're up to."

Police can also use evidence discovered on social networking sites as leverage during interrogations, says Jon Shane, a retired Newark, N.J., police captain who now teaches at John Jay College of Criminal Justice. Investigators can print out a photo from a suspect's Facebook page, showing him at a party at which a murder occurred, and pocket it for when the suspect is brought in for questioning. "When he denies having been at the party, I know he's lying. I already have the evidence in hand," Shane says.

But social media evidence can also be used to exonerate suspects. Dennis Cleary, a criminal defense attorney in New Jersey, represented a woman accused of attempted murder. When the victim testified about her injuries, Cleary was able to contest them because he found evidence to the contrary on to her public Facebook page.

"She said she couldn't go to the gym anymore, she couldn't run anymore," Cleary says. "But she would post from the gym, on her cellphone, that she was on the treadmill."

Tracking Bad Behavior

FOR MONTHS, ABOUT 20 officers in the Toronto police department have been hunting for rioters who disrupted the G-20 summit there last June. Violence erupted after a group of anarchists broke from a peaceful march and

The Digital Arms Race

COPS	CRIMINALS
→ Law enforcement agencies routinely tap into location data from wireless phones during investigations.	→ Drug dealers and gang members use prepaid "burner" phones, then dispose of them before cops can set up a wiretap. These phones have even been found inside prisons.
→ Many police cars have cameras that automatically scan and check the license plates of passing vehicles against databases of wanted criminals.	→ Thieves steal info from credit cards' magnetic strips with portable "skimmers" or via readers installed over legitimate ATMs.
→ A smartphone app called One Force Tracker helps tactical police teams by allowing officers to track one another's positions.	→ Organized cyber-crime networks cover their tracks with antiforensic software such as Evidence Eliminator and Transmogrify.
→ A technology called ShotSpotter uses microphone arrays to allow police to triangulate the location of the shooter in gunshot situations.	→ Car thieves use GPS jammers to prevent systems such as OnStar from reporting a stolen vehicle's location to police.

POLICE TECH/// UNDERCOVER ONLINE

torched police cars, smashed storefronts and looted shops.

Anarchists routinely target G-20 summits, and one of the most potent weapons these groups use to sow chaos is the social-messaging site Twitter. (At the September 2009 G-20 summit in Pittsburgh, anarchist organizer Elliot Madison stationed himself in a hotel room with a view of the street, then tweeted directions to protesters to help them evade police.)

The Toronto investigators had monitored the Twitter feeds of some known anarchists before the conference. Now, says Toronto police detective Mike Jander, the police are friending suspects on Facebook, some of whom used photos of themselves kicking in the headlights of police cars as their profile photos. Thirty people have been arrested to date.

Jander says that for Toronto police, this case is personal. More than 1100 people were arrested during the mayhem that weekend—most of whom were let go—and police faced a barrage of criticism and cries of excessive force. Some working the case have become almost obsessed with finding the vandals, as a matter of honor.

"When you go home, you can't stop," Jander says. "You're on Facebook or Twitter, because you have to see what so-and-so is talking about today. And then a new YouTube video comes out, and you go frame by frame to see who's in the background."

Because of their ability to reach a mass audience instantly, social posting sites enable instigators to assemble "flash mobs" that can quickly turn violent. Last spring, hundreds of teenagers gathered in Philadelphia's City Hall area and began terrorizing pedestrians and employees of area stores and restaurants after they'd received messages about the meeting on Twitter and Facebook.

"We're constantly monitoring them now," said Lieutenant Frank Vanore, a spokesman for the Philadelphia Police Department.

They're not alone. Many departments are now monitoring Twitter and other social media for patterns in the chatter, so they can predict crime—and hopefully prevent it—before it happens. Some law enforcement agencies are beginning to embrace social customer relationship management, or CRM, software, which was developed to monitor chatter from social networks for marketing purposes. Police are using social CRM for predictive analysis, letting the software raise red flags before an outbreak of violence.

Some departments use social media to solicit help from the public in solving crimes, like posting virtual "Wanted" posters. Detectives in Toronto found a murder suspect in 2009 by posting a YouTube video of a detective giving details of the murder and seeking help in finding the culprits. Police had already arrested one man but were looking for the second. Three months after the video was made, a man walked into a police station 30 miles away with information for "the detective on the computer." It took police there 45 minutes to locate an office computer on which YouTube hadn't been blocked. Once they did, they found the video and the name of the detective handling the case. Days later, police arrested the second suspect.

The Party Line

EVEN THE INTERNAL REVENUE SERvice monitors social media. In response to a Freedom of Information Act request by the Electronic Frontier Foundation, the IRS sent the group a 38-page training manual in which it outlines "Internet tools and searches that will be useful in locating taxpayers and determining their online business activity."

Some civil liberties experts wonder whether police are going too far, entering areas for which they might otherwise need a search warrant. Do privacy rights extend to postings on a Facebook page? The answer, according to legal experts, is not really.

Some civil liberties experts wonder whether police are going too far, entering areas for which they might otherwise need a search warrant.

"It's the same as when police go undercover," says Thomas Nolan, an associate professor of criminal justice at Boston University. "This is stuff in the public domain. It's open to public scrutiny. It's a solid, viable means of attaining investigative leads."

Jennifer Lynch, a staff attorney with the Electronic Frontier Foundation, says people should have a reasonable expectation of privacy in their personal communications. But, she adds, "If a person accepts a friend request from someone they don't know and then allows that person access to their private communications, the law is unlikely to find an expectation of privacy."

James continues to pursue her drug kingpin. In 2009, her office began to monitor his associates' cellphones and text messages. Investigators also slipped inside the organization's stash house to do what's called a sneak-and-peek. They found three kilos of cocaine, 16 bricks of heroin, $80,000, two pistols and an AK-47. A few months later, police pounced, rounding up members of the organization. But when they tried to catch the kingpin in the parking lot of a shopping mall, he took off, vaulting over a fence and an eight-foot wall, then disappeared into traffic.

Last year, James heard that one of the drug dealer's friends was sending encoded messages from his Facebook page to let people know the kingpin was all right, but she went to that page and found nothing. What she really hopes to find is the dealer himself, lurking, like her, behind some false online persona.

"He's sneaky. There's no way he'd use his own name on Facebook," James says. "But I scroll through his friends' lists looking for things like his son's name, which is unique." James hasn't found him yet, but she's confident that he'll eventually rejoin the online conversation. **PM**