OFFICER.com

High-Tech Stalking

Christa Miller

Updated: April 30, 2009

When they hear the term "stalking," many people think of an obsessed fan standing for days outside his or her favorite star's house. But stalking affects a variety of people in many life situations — and in recent years, has gone high-tech. Disgruntled employees pose as their bosses to post explicit messages on social network sites; spouses use GPS to track their mates' every move. Even police and prosecutors find themselves at risk, as gang members and other organized criminals find out where they live — often to intimidate them into dropping a case.

Federal stalking statistics

In January, the Bureau of Justice Statistics released the largest-ever study of its kind on stalking, "Stalking Victimization in the United States," an Office on Violence Against Women (OVW)-sponsored report based on supplemental data gathered from the National Crime Victimization Survey.

The report showed that technology, including Internet-based services like e-mail and instant messaging along with other technology such as GPS and computer spyware, have been used to harass one in four stalking victims. That translates into about 1.2 million victims whose stalkers used some form of technology to find them.

However, law enforcement remains under-equipped to deal with stalking. When it comes to technology use in the crime, the problem worsens. There are many reasons for this, but the end result, as revealed in the survey, is that victims have mixed feelings about police response to their problem.

Mixed police response

Stalking has always been difficult for law enforcement to deal with. For one thing, says Michelle Garcia, director of the Stalking Resource Center at the National Crime Victims Center, stalking is a relatively young crime; the first anti-stalking law was enacted in California in 1990. "The behavior may be as old as society, but the crime itself is less than two decades old," she explains.

While all 50 states have passed anti-stalking laws, only 14 of them specifically address high-tech stalking. The laws overall are inconsistent with how they address the crime. Some require the victim to feel in fear of his or her life, while others allow that any "reasonable person" would feel threatened.

In addition, stalking is unique in that it involves a pattern of generally noncriminal behavior rather than a single incident. Officers may believe they are taking a report on a single incident, therefore, may believe it's a waste of time. And training them otherwise is unusual. "Many departments have no specific training, no specialized units that deal with it," says Garcia. "When officers do encounter stalking, they are often uncertain about how to respond because they haven't been trained for it." Academy training, she points out, may provide recruits with a 4-, 6-, or 8-hour education on crimes against women. "Stalking may be just one small piece within the larger topic of domestic violence and sexual assault," Garcia adds.

Information sharing — or lack thereof — among agencies can be another part of the problem. "Many state laws require two or more acts against a victim to qualify as stalking," says Garcia. "But a victim may work in one town and live in another. If she receives dead roses at work and multiple phone calls at home, and reports each event to each police department, neither one will have enough for a crime if they aren't working together."

The high-tech element can present an extra wrinkle. "Some agencies are well trained on stalking and domestic violence, but they have no specialized computer forensic unit or investigator. Others have high-tech crimes units, but little experience with stalking," says Garcia.

Stalking, with or without technology, can be such a complex crime that many police officers, detectives, prosecutors and others in the criminal justice system become frustrated. Sometimes this comes out as negative attitude toward victims. But Alexis Moore, founder and president of the national victim advocacy group Survivors In Action, believes this can be overcome. "Nothing is truly complex, but it can be if it's allowed to be," she says.

Key to understanding and investigating high-tech stalking are training and education; collaboration, including information sharing; and developing standard protocols for how to work with victims.

For investigators

Investigator Sgt. Mark Wojnarek, who has commanded the Special Victims Unit (SVU) of the Montgomery County Sheriff's Office (MCSO) in Tennessee since 2003, says high-tech tools have become so ingrained in society that it's important to assume victims and suspects have one or more. In fact, his detectives conduct a technology risk assessment asking victims: How many computers are in the house, who has access, whether vehicles are equipped with GPS, how many cell phones and so on.

Also important to understand are basic facts about high-tech stalking. For one thing, Wojnarek says there is no "typical" victim or perpetrator. "It's everyone," he says. "Juveniles, men, women."

Resources can be a delicate balance. Budget troubles may mean that even departments with domestic violence specialists will have to assign other duties to those investigators, or assign domestic violence and stalking cases to investigators untrained to deal with them. And even before the recession, computer forensics and high tech crimes labs were severely backlogged. Yet so much of this type of evidence is so volatile, says Moore, that evidence can disappear within a matter of months — even weeks.

Rural MCSO's answer was to train its SVU detectives to deal with high-tech tools themselves: To solve the problem — the kind of crime — using specific tools, in this case the recovery of computer and mobile device evidence.

Wojnarek says the legacy "stalk the stalker" model that had police sitting in unmarked cars watching suspects is "archaic." And unlike detectives who trace child predators online, investigators who deal with high-tech crimes are better served to get out in the field than to sit behind a computer. "Our best tools these days are the search warrant and strong investigative techniques," he explains.

For patrol officers

Generally, says Moore, "traditional" stalking is the first behavior that victims notice and report. "Stalkers turn to technology when they don't get what they want," she explains. So, foremost, officers need to be trained on stalking behavior, including instruction not to treat it like other single-incident crimes.

One problem: Officers don't know the right questions to ask. "It's not about behavior, or the stalker's date of birth or Social Security number," says Moore. "It's about the IP address, the Internet service provider. Stalkers actually make it easy for you to find them because they keep attacking."

Many victims will be too scared or confused to deliver such information right away, so officers need to help them collect it or teach them how to ask tech-savvy family members or friends to help. Throughout the process, they should be working from a strong protocol. As Wojnarek says, officers should not bear the burden of investigation. MCSO deputies, for example, know they have a unit to call on for help. "We tell them we'd rather come out and not find anything, than not go and end up with a dead victim," he says.

Officers are instead trained on how to "notice" things when they respond to domestic calls. For instance, says Wojnarek, "if the victim says her spouse repeats conversations back to her verbatim, that's a sign there's a listening device in the home." Training on this kind of recognition takes place quarterly, along with regular bulletins on domestic violence trends.

The MCSO SVU also presents to schools, elder homes, and the local domestic violence coalition. "Safety planning now needs to include high-tech tools," says Moore, who believes all this will be easier as time goes on. "Most young officers will understand how technology can be used to stalk because they themselves use it," says Moore. "They're aware of the pitfalls [with privacy], so it's possible to tweak that awareness to help them understand the way criminals use it."

Training and education

Moore says many police departments' domestic violence training is woefully out of date. "They're still using material from the 1990s," she explains. "It references cases like Nicole Brown's. Technology has gone far beyond that — it changes by the hour, not by the year."

Wojnarek says law enforcement is always likely to be out of date. "Technology is moving so far and so fast. But that doesn't mean agencies can never be equipped to deal with it." His unit receives ongoing training on domestic violence, sexual assault, and like issues from a variety of sources.

One of them is the Stalking Resource Center. Garcia says, "We are funded to provide training and technical assistance to any agency that receives USDOJ Office on Violence Against Women grant funding. We are able to come to them at very low, or no cost." In fact, says Wojnarek, the Stalking

Resource Center has been his unit's greatest help, to the extent that MCSO detectives are now qualified to train on the Center's behalf.

He adds that training and education are important to agencies and victims alike. "Even if you can't afford a unit, officers need to be educated to look for certain things they may not otherwise have looked for," he explains. The first case Wojnarek worked after his training was a stalking case involving Spector spyware — which he says he would've thought was just a video game if he hadn't had the training.

Investigators can also educate themselves via the Internet: Becoming active on detectives' forums and listservs, for instance, or even learning from the same places the stalkers do. Just as pedophiles learn from and empower each other online, so do stalkers. Moore says it's good to learn to think like they do. "Your mind has to be able to warp and tweak information to figure out what perps are doing, and can do, with the technology," she says.

Education often goes hand in hand with information sharing. As investigators from one department involve other agencies, they find they must teach investigators and officers about what they're doing. Wojnarek says this can be hit or miss. "Technology intimidates many people in law enforcement," he explains. "Even something we think of as simple, like tracking cookies, scares a lot of cops. It's like a language barrier: They can understand the words, but not the context."

This is also a problem within the criminal justice system. Prosecutors and judges have a hard time understanding the issues, much less explaining them to juries. The inconsistencies within state laws make it worse. "The language is outdated when it comes to high-tech stalking," Moore explains. "Even when high-tech crimes units are able to do good work, cases are often [pleaded] out because prosecutors don't understand the nature of the offenses they are dealing with."

High-tech stalking is a complex problem, but will continue to evolve along with technology. While law enforcement agencies may need to take baby steps to learn about and deal with it, enabling officers and investigators to do so will lay the foundation for future improvements and understanding — for everyone involved.

Editor's note: The Bureau of Justice Statistics' Special Report, which includes statistics on high-tech monitoring in stalking and harassment cases, is available at **www.ojp.usdoj.gov/bjs/pub/pdf/svus.pdf**.

Christa Miller, a New England-based freelance writer who specializes in public safety issues, can be reached at ***christammiller@gmail.com***.