Officer.com

April 2006

Cyber Stalking & Bullying – What Law Enforcement Needs to Know

By Christa Miller

Cyber stalking and bullying are two new takes on old threats. While the Internet is the weapon of choice, it's far from harmless. Just as more "traditional" stalking and bullying can escalate to physical threats – including murder and suicide – so can their cyber forms.

The problem is, many police departments remain unable to investigate and solve these cases. However, the good news is equipment and technology aren't always the answer. Training, education and a willingness to collaborate are.

Limitations in Police Response

In 1999, the U.S. Department of Justice (DOJ) documented that, "while some law enforcement agencies are responding aggressively, others are not fully aware of the problem and lack the expertise and resources to pursue cyber stalking cases." Parry Aftab, an attorney whose pro bono work includes WiredSafety.org and its related sites, agrees. "Many small-town officers, when confronted with an upset parent, don't know what to do," she says. "They can't handle the complaint because they lack the technology, and they can't advise the parent on what to do because they don't know the laws. Often, they encourage the victims to ignore the abuse, even if it requires intervention, because they're embarrassed to say they don't know how to handle it." She believes small-town officers have the greatest need for training and education. "More kids are online in small towns because they're looking for something to do," she says.

One potential barrier to effective law enforcement response is individuals' perceptions. "Many people who understand offline bullying think cyber bullying is the same thing, but it is not," says Aftab.

According to the National Center for Victims of Crime (NCVC), cyber stalking is "threatening behavior or unwanted advances directed at another using the Internet and other forms of online and computer communications." Cyber bullying is similar to cyber stalking but draws its distinction through demographics. Instead of adults targeting other adults or children, cyber bullying involves minors targeting minors.

Another problem is technology itself. "It's not enough to have the victim print an e-mail," says Aftab. "You must be able to trace the header. However, many older street cops are not tech-

savvy, and younger tech-savvy people are more likely to work in the private sector than they are to go into law enforcement."

Another obstacle is lack of funding. Jay Fisher, director of the Cyber Crimes Unit at CyberAngels.org, says that because cyber harassment itself is a relatively new crime, federal funds don't yet exist to help agencies combat it.

Funding is always an issue, agrees Jim Batelli, Mahwah, New Jersey, chief of police. This leaves law enforcement responsible to garner public support for more funding. "Sometimes it takes a high-profile case where a child is abducted before the public stands up and mandates public officials to take action. Unfortunately, by that time it is too late for the victim and his/her family. Simply put, police agencies must proactively obtain training for their officers. A reactive police agency is ineffective in today's society; citizens deserve and demand better."

Publicizing the problem can help an agency gain community backing. "You must be willing to discuss the problem's severity, to let people know it exists in every community regardless of size," Batelli says. "The Internet has no boundaries. It is not limited to inner-city or low-income families. It exists in every community. It is an easy, anonymous and quick medium for predators to use."

Training and Education

To educate law enforcement officers, WiredSafety.org partnered with a Canadian group to produce a CD-ROM containing both school resource and community-oriented policing resources. Agencies also can send officers to training offered by various law enforcement groups around the region or country. "It costs, but we view it as our obligation," says Batelli. "Often it's the only way we can get good education." He adds that often training that covers one subject – such as identity theft – can be applied to cyber stalking or bullying investigations.

Otherwise, says Fisher, it's important for individual officers to be comfortable using computers. This includes veteran officers. "The older generation tends to be in management and sets the agenda," he notes. "As they spend more time online, they will see the Web's scope and its criminal potential. This will help them shift their focus and priorities."

An important part of any agency's cyber crime prevention strategy should be citizen education. WiredSafety.org offers free manuals, Microsoft PowerPoint presentations for school resource officers to show, handouts and other materials. The organization even recently entered into a licensing agreement with Marvel Comics. It can use Marvel's characters in a series of custom comics that will teach kids about cyber bullying.

Agencies also can follow the lead of groups such as CyberAngels.org, teaching citizens how to protect themselves. "We will suggest methods for people to go 'anonymous' on the Web – changing identity, placing firewalls [and other off-the-shelf security], etc. A person can get decent Internet security for a price." However, he adds, cyber stalkers and bullies often attempt to test these products' limits. Thus, police must still be ready to respond to cyber harassment incidents.

Legalities

A critical aspect of understanding cyber harassment is knowing what legislation covers, and what it does not.

The federal Violence Against Women Act, passed in 2000, includes cyber stalking in its interstate stalking statute. However, because this is the only federal anti-cyber stalking legislation available, most states have had to define the crime further. The NCVC notes that most states' anti-stalking laws cover cyber stalkers' behavior. While some have revised their statutes or enacted laws specifically to include computer-based harassment, others have written their anti-stalking language broadly enough to include both online and offline offenses.

Cyber bullying is a different legal matter altogether; most of it is covered by the First Amendment. "Rude and horrible speech is not illegal in the United States," says Aftab. "It can't be criminalized unless, and until, it falls outside the First Amendment's bounds." No legal test defines cyber bullying. "You know it when you see it," Aftab says.

Clear-cut crimes take place when a would-be bully says or does something that may get adults involved, such as "offering" a victim to an adult offline. "In those cases, law enforcement must get involved," Aftab says.

Responding to Cyber Harassment

In Mahwah, police handle a cyber harassment complaint much like any other – the first responding patrol officer forwards the initial incident report to detectives. Then, the decision is made whether or not to assign it to an investigator for follow-up. The department's school resource officer follows up on any cyber bullying complaints in the schools. "Fortunately, all our investigators have some Internet safety investigative techniques, although it is an ongoing process," says Batelli. "In some instances we may contact the county cyber crime task force, but we try and handle most cases in-house."

Batelli believes enough time and effort can resolve nearly every incident. For one thing, prosecution isn't always the answer. "We work closely with victims to decide which avenue they are going to take," he adds. One alternative is civil court. The burden of proof is less than in a criminal case, and victims can recoup losses owing to humiliation, slander or libel, or related torts.

Most importantly, says Batelli, police must place high priority on cyber harassment. "Predators often use fear," he says. "The mission of law enforcement agencies is to provide their citizens with a sense of security and freedom in their homes. If an agency cannot handle its caseload, it must be willing to pass it on to another agency that has the necessary [prosecutorial] jurisdiction."

Even if agencies can handle their caseloads, the nature of cyber harassment often requires collaboration. "We work very closely with community groups, parents, educators, businesses and school organizations to get our message out," says Batelli. "These outside groups can provide

funding and resources that may otherwise not be available to law enforcement agencies. No one group can do it alone, but together they can form a formidable opponent."

Working with ISPs

The DOJ acknowledged in 1999 that Internet Service Providers (ISPs), similar to law enforcement agencies, provided mixed results in both preventing cyber crimes and helping victims respond. Aftab says some ISPs, such as Microsoft and America Online, are very proactive with regard to online abuse and will work extensively with police to halt and prevent it. "Even a small agency should not have a problem working with large corporate ISPs," she adds. Other, smaller ISPs may need just as much training as police; WiredSafety.org can provide it.

In general, Aftab says ISP involvement can be very effective against some cyber bullies, especially when it involves rescinding their Internet access. However, because this only covers one aspect of cyber bullying, WiredSafety.org is working with blog (online journal) hosting services. Custom-designed guides will help these services aid law enforcement in investigating cyber bullying. In exchange for WiredSafety.org's safety tips and other support, services like MySpace, Blogger, Facebook and Piczo agree to rewrite privacy policies, store user information (including entries) for 90 days and cooperate with law enforcement - to the extent of requiring no subpoenas in emergency situations.

Working with Schools and Parents

Schools and parents can become very effective allies in preventing and ending cyber bullying. This is especially important in a noncriminal case; bullies need consequences for their actions. However, schools can be sued for disciplining students over actions that take place off school grounds.

Aftab recommends a two-pronged approach for schools, which law enforcement agencies can help with:

1. Educate students on cyber ethics and laws.
2. Make cyber bullying a contractual issue. Via their acceptable use policy, schools can reserve the right to discipline for off-campus actions that intend to affect a student's in-school safety and well-being.

Apart from these solutions, Aftab says community outreach is key to preventing and ending cyber bullying. "Law enforcement officers can act as mediators between bully and victim," she says. "WiredSafety.org also crafts community service programs for bullies, such as having them create a presentation to offer in their schools." Such programs can be very effective; Aftab notes that several bullies have reformed to the extent that they can join TeenAngels, a branch of WiredSafety.org composed of police-trained teens who educate fellow students and their parents about online safety, privacy and security.

The Mahwah Police Department has sponsored a TeenAngels chapter since 2005, after Aftab made a series of appearances before schools and parents. "I recommend a TeenAngel group to

any law enforcement agency," Batelli says. "Since it is hosted by police, it breaks down barriers between law enforcement and children, which always has positive results."

Working with Online Groups

Law enforcement officers have allies in groups such as WiredSafety.org and CyberAngels. Most significantly, these groups can intervene in First Amendment situations where law enforcement agencies, as part of the government, cannot. "As CyberAngels is a private organization and the victims are private citizens, we do not labor under the same constraints," says Fisher. "CyberAngels will likely remind Web site hosts [on which harmful content is posted] that they cannot let users 'yell fire in a crowded theater.' We also will remind them that they may be civilly liable in the event a victim is harmed because of material posted on a site."

These groups also can assist law enforcement agencies in putting together investigations. "Our Cyber Law Enforcement Division, which is composed of volunteer active and retired law enforcement officers, will help them figure out what evidence they need to collect, how to collect it, where to send a subpoena, and how to evaluate the risk," says Aftab. "We train them in what cyber abuse looks like and where to go for help." The division's staff also helps law enforcement officers make contacts outside their jurisdictions, when necessary. "We reach out to federal Internet Crimes Against Children (ICAC) task forces, state police high-tech crime units, even Interpol," Aftab adds. "Small agencies don't have those relationships, so we do it as a favor." CyberAngels will soon offer a related service: the Police Liaison Unit (PLU).

CyberAngels' function is similar. "We have an 'ad-hoc' way of working with law enforcement," says Fisher. "If a victim contacts us before seeking help from the police, we will pursue the matter as much as possible before recommending police assistance. However, if there is an immediate threat for potential physical violence, we will recommend immediate police intervention. [On the flip side,] if police refer a victim to CyberAngels and we solve the victim's problem, we saved the police time and effort. Even if we see something serious, we can refer the matter back to police with an initial investigation done to highlight the seriousness."

Third-party groups can offer victim services, which law enforcement agencies may not be in a position to do. Sometimes victims come to CyberAngels who have received an unsatisfactory response from the agencies in their hometowns. "We will assist these people to the fullest extent possible, and then recommend alternative law enforcement agencies for them to contact," Fisher says. CyberAngels also advocates for victims, and can help them pursue civil suits.

Both organizations are just a phone call or e-mail away. "Officers can call me with whatever they need to," Aftab says. "There is no 'process' to go through."

Looking Ahead

State and regional computer crimes task forces continue to be overburdened. Batelli believes local agencies must take the initiative to train their officers to handle cyber threats. "Police have to be innovative to combat Internet crime, because the predators certainly are," he says. Part of this innovation is publicity that can attract lawmakers' attention. "Legislators must get involved

in enacting practical laws and enhanced penalties for offenders that use the Internet for crime. An effective response from law enforcement and the legislative branch is critical."

The good news, Fisher believes, is that computer skills are easy for police to acquire. "One person with a decent system who is knowledgeable of both software and operating systems can be very effective – as effective as some task forces," he says. "If no one is working on computer crime in a major city, that city suffers. If one cop in a small town is a tech genius, that town will likely have great cases built against online criminals."