The New Age of Stalking: Technological Implications for Stalking

By Cynthia Fraser, Erica Olsen, Kaofeng Lee, Cindy Southworth, and Sarah Tucker

ABSTRACT

Technology has led to tremendous advancements in our society but has also brought more danger to victims of stalking and given more tools for stalkers to use. New technology has made it more difficult for prosecutors and judges to hold stalkers accountable for their crimes, and without an understanding of how technology is misused by stalkers to track and monitor their victims, many victims don't get the justice they deserve. This article addresses the tremendous impact of technology on stalking, especially within the context of intimate partner stalking.

The motivations and techniques of stalkers have remained remarkably consistent over the years. The tools stalkers use, however, have changed over time. In the past, a stalker may have lurked outside the victim's home, waiting to follow her. Today, he[1] can purchase a location tracking device and attach it to her car. Once attached, the stalker can monitor the tracking device from any cell phone or computer with Internet access; he can watch a map on his screen and track her car from location to location throughout the day.

Stalkers exploit technology and use it in ways that the creators never intended or envisioned. Technology has given stalkers new tools, enabling them to reach their victims from afar while infiltrating even deeper into their victims' everyday lives. Stalkers take

1 Generally, stalkers are male (79%), victims are female (75%), and stalking is often perpetrated by current or former husbands, boyfriends, or cohabitating partners (Baum, Catalano, Rand, & Rose, 2009; Spitzberg, 2002). For the purpose of this article and within the context of stalking in intimate partner violence, we refer to the victim as female and the perpetrator as male. Although women are significantly more likely to be victims, they can also be perpetrators; likewise, although men are more likely to be perpetrators, they can also be victims of stalking. Men are more often stalking victims in gay intimate partner violence or in situations where a male not only stalks an ex-girlfriend but also her new boyfriend.

The authors, with more than 60 total years of experience in the field of domestic violence, make up the Safety Net Project at the National Network to End Domestic Violence (NNEDV). **Cynthia Fraser, Erica Olsen, and Sarah Tucker** are Technology Safety Specialists; **Kaofeng Lee** is Project and Communications Specialist; and **Cindy Southworth** is founder of the Safety Net Project and Vice President of Development and Innovations at NNEDV. Correspondence: cs@nnedv.org

away a victim's sense of privacy, control, security, and safety, and create an atmosphere where the victim feels like the stalker knows everything she does and says. The sense of isolation and fear deepens when victims feel that no one believes them because the stories they tell seem impossible.

Because the stalking is more stealthy, victims become suspicious only when the stalker seems to know more than he should; victims often do not know how the stalker is doing what he's doing. It is important, as a result, for professionals to understand how surveillance, tracking, and eavesdropping can be done with commonly used technology. While some stalkers use specialized devices, most stalkers modify or manipulate everyday technology that the victim is already using, such as phones and computers. The ever-changing nature of technology requires constant attention and education so professionals working to bring justice to victims can do so effectively, with a thorough understanding of how far technology has come.

While technology has made it easier for stalkers to harass their victims, technology has also made it easier for the criminal justice system to hold stalkers fully accountable—by charging and convicting stalkers for criminal actions that might have been more difficult to prove in the past. Stalking incidents are often no longer "he said, she said" cases; law enforcement can corroborate a victim's experience of stalking by using technology to collect timely evidence. For example, if the stalking includes text messages, law enforcement can review the victim's cell phone records, as well as gather evidence from the stalker's cell phone or service provider to document that the stalker sent the harassing text messages to the victim.

STALKING AND TECHNOLOGY: SAME BEHAVIORS, NEW TOOLS

Technology stalking often is described as "cyberstalking;" however, the term does not fully describe the wide range of ways stalkers misuse technology. The term "cyber" implies something that occurs only on the Internet. For many victims, the stalking is a combination of stalking via the Internet and other technological tools, as well as in person.

Over the last 20 years, Americans have transitioned to an increasingly digital society, and by the end of 2009, 74% of adults were using the Internet and 89% of adults were using cell phones (CTIA The Wireless Association, n.d.; Rainie, 2010). As the public use of new technology increased, so did stalking cases involving the misuse of technology. States soon began amending their stalking laws to add a prohibition against "electronic communication or contact," and federal and state electronic privacy and wiretap laws increasingly became applicable in stalking cases. Indeed, Section 2261B of the federal Interstate Stalking Law forbids the use of regular mail, e-mail, or the Internet to stalk another person across state, tribal, or international lines (18 U.S.C. § 2261(b)).

It is often believed that new technologies create new criminals and new types of crimes. Yet, it is important to remember that stalking existed before the development of

the computer, Internet, or cell phone. The danger with technology, however, is that it gives stalkers additional tools to use and can enable their tactics to become much more invasive.

Although research on technology stalking is minimal, there is research that shows that more than one in four stalking victims reported that their stalkers used some form of technology (Baum et al., 2009). Of those who reported being stalkers electronically, 83% reported being stalked through e-mail and 35% through instant messaging. Additionally, 46% reported that the stalker used a hidden camera to monitor their actions, and 10% reported that Global Positioning System (GPS) location tracking technology was used to monitor their location (Baum et al., 2009).

As each new technology evolves, it becomes easier for perpetrators to stalk their victims. Computer monitoring software can track and record every keystroke a person makes on a computer. Location tracking devices, such as GPS, can track victims' daily movements and their real-time location. Hidden cameras and audio bugs have become much smaller and more affordable so it is easier for stalkers to install surveillance devices inside a victim's home, car, or workplace. Every year brings newer and better technology that intimate partner stalkers can misuse. A stalker can now harass a victim or her friends and family by faking his voice over phone calls or falsifying the phone numbers displayed on Caller ID when sending text messages. Stalkers can even send threatening e-mail messages that "disappear" from the victim's e-mail system after they are read.

Stalkers are using technology to harass and instill fear because it's available and relatively inexpensive. For less than $100, a stalker can purchase computer monitoring software, commonly known as spyware, remotely install it on a victim's computer, and monitor everything that occurs on the computer, from keystrokes typed to Web sites visited to documents read or edited (one example: www.spectorsoft.com). Furthermore, as victims increase their use of technology, it becomes one more aspect of a victim's life that a stalker will try to control. Often, stalkers log on to or hack into a victim's e-mail account to read messages, leave veiled threats, or even send e-mails that look like they came from her.

While some technologies can greatly facilitate evidence collection, other technologies have made it more difficult for law enforcement and victims to prove the identity of the stalker. Unfortunately, some victims may experience the stalking and harassment for months before they have the type of evidence that causes law enforcement to decide to investigate further and move forward with a case. Law enforcement will sometimes have a very short timeframe to investigate and obtain enough evidence to press charges. Stalking can be so complicated that law enforcement may focus on other charges or elements of the case, and the stalking may never actually be charged or brought before a prosecutor.

How do victim advocates, service providers, law enforcement, and the justice system address the dangers and safety risks of these new technologies, keep victims safe, and hold stalkers accountable? The first step is to understand how the technology is being misused. The next section of this article will describe the tactics and common technology tools stalkers misuse to monitor and harass their victims.

Repetitive Contact Via Technology

One of the more obvious forms of technology stalking or harassment is constant contact via technology. Stalkers will sometimes make hundreds of unwanted phone calls, while also sending text messages, instant messages (IM), or e-mails to the victim. This harassing contact is common in dating violence, particularly with teenagers; a perpetrator will continue texting or calling until the victim responds. Victims will sometimes change their phone numbers, e-mail or IM accounts, or block the stalker from calling, texting, or e-mailing. In many cases, the stalker will obtain the new number and continue to call or text. Some victims will simply screen their calls and not take a call when they recognize their stalker's phone number in the Caller ID. Unfortunately, the perpetrator may circumvent such blocking by just using another phone.

Repetitive harassing and unwanted calls can be terrifying and disruptive for victims. The initial fear, compounded by the dread that the harassment will never stop, creates a scary reality for any victim. Sixty-six percent of stalking victims report receiving unwanted phone calls and messages (Baum et al., 2009).

Some stalkers use prepaid cell phones, purchased at discount or electronics stores, to make anonymous calls. Prepaid cell phones usually do not require a long-term contract or any personal information to activate. Although prepaid cell phones make it harder for law enforcement to track the phone and connect it to the stalker (as opposed to a traditional cell phone plan with a wireless carrier), it can be done. In some cases, investigators have obtained the call records for a particular prepaid phone and ultimately linked the calls to a suspect (Baker & Shane, 2010). In other cases, investigators have obtained records that show the date and time the phone was activated and even the retail store that sold the phone. Law enforcement officers have then reviewed store security camera footage that connects the stalker to the purchase of the device (personal communication with Detective D. Fishel, October 27, 2009). In addition, reviewing the stalker's credit card account or receipts may reveal purchases of prepaid cell phones or prepaid minutes. Furthermore, each prepaid carrier has its own procedure for activating cell phones and may have information on their users (Jansen & Ayers, 2007).

Now there are new tools stalkers can use to conceal the phone number from which the call originated. Victims may suspect that it is a former or current partner making the unwanted calls, but may be unable to prove it because the phone numbers originating the calls are random, unknown, or may even appear to be the phone number of a friend or family member. Stalkers also commonly use "spoofing" services, which are widely available on the Internet (Jordan, 2010). Spoofing services mask the caller's phone number on Caller ID, making the victim think she is receiving the call from someone else. One type of spoofing service, SpoofCard (www.spoofcard.com), gives callers the ability to fake the number they are calling from, allowing the caller to enter any number he wants to be displayed on Caller ID. SpoofCard even gives callers the option to record the call and fake their voice to sound like a man or a woman.

Currently, spoofing services can be an investigative challenge because the spoofed (fake) phone number will appear on Caller ID as well as on the itemized phone bill of the person who was called. Investigators can find evidence that the stalker used a spoofing

service by reviewing the stalker's phone records, which may document the toll-free numbers used when making these calls through the spoofing service. Investigators can also subpoena the records of the spoofing company to see calls that came into their service during a specific timeframe. The spoofing company may also store additional information about the customer, such as credit card or PayPal account numbers, which would assist law enforcement in connecting the stalker to the harassing phone calls. Additionally, if a stalker tries to use a spoofing service to create a false evidence trail and brings in his phone records claiming the victim is "really stalking him," this false trail can be easy to unravel; the victim's phone records can show that her device never made these calls. The victim may also have witnesses who can corroborate that she was doing other things (e.g., in a meeting) when these fake (spoofed) calls were ostensibly made.

As of May 2010, both houses of Congress have passed versions of a bill which makes it illegal to transmit false Caller ID information with the intent to deceive or defraud (Truth in Caller ID Act, H.R. 1258, 2010; S. 30, 2009). If the bills are reconciled, passed, and signed into law, U.S. attorneys will have an additional federal charge available for use in stalking cases.

In addition to being harassed by phone calls and voicemails, victims of stalking often report unwanted text messages (BBC News, 2003; Smith, 2009). Again, to help mask their criminal behavior, stalkers may use services that allow them to send anonymous text messages. Stalkers can send text messages through cell phone company or third-party Web sites, where the sender can enter any name and phone number he wishes. Texts can also be sent to landline phones; the victim will receive a voicemail of the text message read aloud by an automated voice.

Unwanted e-mails are also a common stalking behavior; 30% of technology stalking victims report receiving unwanted e-mails and letters (Baum et al., 2009). Of victims who report that their stalker used electronic means, 83% reported being stalked via e-mail (Baum et al., 2009). Proving that a harassing e-mail is from a stalker may be difficult since stalkers can create multiple e-mail accounts.

In an effort to delete evidence before investigators can trace it back to stalkers, there is new software that promises to delete e-mails from the receiver's inbox. "Disappearing e-mail," marketed as a "great way to tease or have fun, with the peace of mind that it will not come back to haunt you" (www.selfdestruct.com, 2010), will vanish or "self-destruct" after being read. Other services (such as self-destructing-email.com or kicknotes.com) offer additional "tracking" features that will inform the sender of when attachments are opened, if they are forwarded, and the location of the e-mail recipient (determined by the computer's IP address). Similarly, there are products that promise text messages will disappear from the receiver's phone after a certain period (see www.tigertext.com).

In an effort to discredit the victim or have charges pressed against her, some stalkers use these products to send themselves threatening messages. However, it is possible for investigators to trace the messages, whether e-mail or text messages, to the true sender. In most cases of e-mail harassment and stalking, e-mails can be traced back to the computer from which they were sent. E-mail headers contain unique Internet Protocol (IP) addresses that record which servers the e-mail traveled through to get from the sender to the receiver. After getting the sender's unique IP address, law enforcement can

identify the Internet service provider and then obtain records to determine which computer used that IP address at the time the harassing messages were sent. If the stalker used his computer, it would be traced to him. If the stalker used a computer at a library or a friend's house, investigators will have to take more steps to make the connection between the stalker and the computer used to send the messages.

Using IP addresses to determine who sent an e-mail will not work if the sender uses an e-mail anonymizing service. An e-mail anonymizing service will block the IP address from which the e-mail originated, requiring investigators to track down records from other sources, such as the abuser's e-mail records.

Regardless of the tactics used, it is important to view the acts as part of a pattern of stalking behavior. Depending on the case and specific history, 50 text messages a day may be as scary to one victim as a single text message threatening the victim's life. Furthermore, stalkers have so many ways to hide or anonymize themselves when sending threatening messages or calls, a victim could receive 50 hang-up calls from 50 different phone numbers a day or receive text messages that disappear from her e-mail or cell phone.

Surveillance and Tracking

One of the more terrifying tactics used by stalkers is to make the victim feel that she has no privacy, security, or safety, and that the stalker knows and sees everything. With technology, it is not difficult for stalkers to appear omniscient. Cameras can assist stalkers in monitoring victims in their homes or workplaces, GPS devices can track victims wherever they go, and audio surveillance can record victims' every conversation.

Stalkers have used hidden cameras to monitor activities inside a victim's home. Often called "nanny cams," spy cameras can be hidden inside everything from children's toys to clock radios to potted plants. Some stalkers can remotely activate the victim's computer's webcam to watch or listen in on whatever's happening. Other stalkers take advantage of the remote access features in complex home security systems, using their cell phones or laptops to view security cameras, turn lights on and off, reset the thermostat, and more.

Stalkers can use the GPS function on a cell phone to obtain and track a victim's location in two ways. The first is to use a "friends and family" or "child locater" service offered through the cell phone carrier. To activate these services, the stalker needs access to the victim's account. Because many intimate partner stalkers have either shared a cell phone plan with the victim in the past or have the correct information to appear to be an authorized account holder (generally a Social Security number or billing zip code), pretending to be the victim to authorize changes to her cell phone service isn't usually a major obstacle. However, most carriers now automatically send a text message or e-mail notifying the account holder that changes have been made to her account.

The second method stalkers can use to track victims is to install a third-party application that uses the GPS capability in a cell phone. Some GPS tracking applications designed by third parties don't always offer safeguards, such as notification, so stalkers who have physical access to the victim's phone may install a GPS tracking application on

the victim's phone without her knowledge. The stalker can then log on to a Web site and follow the location of the victim in real-time.

In a 2004 California case, a stalker purchased a cell phone, activated the GPS locater service on the phone, and hid the cell phone on the victim's car. The stalker was caught when the victim saw him under her car trying to change the cell phone's battery (Boghossian, 2004). In another case, a Washington stalker hid a phone behind the victim's dashboard and wired it into the car battery, using the car to charge the cell phone (Donovan & Bernier, 2009).

Stalkers can also use GPS devices created specifically for tracking. Companies with large fleets of vehicles (such as package delivery firms) often use tracking devices to monitor their vehicles or goods. Many tracking devices are very small and can be easily hidden, sometimes embedded in watches or in USB memory sticks. Furthermore, many cars now have navigational systems. Some services, such as OnStar, will release information about a car's location to whoever is listed as the car's owner. In cases of intimate partner stalking when a couple is separated, the listed owner of a car could be the stalker, even if the victim is driving the car.

Some of the monitoring devices stalkers use are legal to own and use (and are marketed to parents or employers to monitor their children or employees). For example, depending upon state law, it may be legal for the stalker to purchase a GPS tracker and to place that tracker on a vehicle the stalker owns. However, stalkers are using the monitoring devices in illegal ways. In these situations, the focus needs to be on the stalker's illegal behavior. Purchasing, owning, and even using monitoring devices may be legal, but when the devices are used to stalk another person, the stalker can be charged with a crime.

A common underpinning of all stalking cases is the stalker's obsessive need to know everything the victim does. With the advent of wireless technologies, stalkers have adopted new tools to gather this information; however, they have not stopped using traditional tactics and older tools, too. In 2002, one man intercepted his ex-girlfriend's landline phone calls by splicing the wires in her basement phone box and attaching them to a tape recorder he encased in a backpack and left leaning against the foundation of her home. He was arrested when he went to retrieve the backpack (Miller, 2003). In another case, a stalker broke into the victim's home to read the numbers on the Caller ID, just to know who she had been talking to (Ohlson, 2003).

Stalkers can also install spyware onto a cell phone to turn a phone into a listening device. Some additional features of spyware on a cell phone include the ability to see the text messages a victim sends and receives, eavesdrop on phone calls and voice mails, receive satellite updates on the victim's (or the phone's) location, and view the ID of all incoming and outgoing calls. At this time, most cell phone spyware can only be installed by having physical access to the victim's phone. Once installed, however, the victim will have no clue that the spyware is running except for signs that the stalker knows more than he should, and possible increases in data or phone charges on the victim's phone bill.

As more and more people use their computers to work, pay bills, and connect with friends, a person's computer activities can contain a wealth of personal information. One of the most common ways for stalkers to spy on their victims is to install spyware on a

victim's computer. Spyware, initially marketed as a type of "Net Nanny" to monitor children's online activities, has quickly become a product used by employers to monitor employees and by spouses to monitor their partners. In fact, some products are specifically marketed to "spy on your spouse" (www.e-spy-software.com).

Stalkers can remotely install spyware on a victim's computer by tricking the victim into opening attachments, such as a photo, game, or greeting card. In fact, victims may be unaware that the e-mails are from the stalker since he can use a false e-mail address. Such was the case in Illinois where a police officer tricked his ex-girlfriend into opening a spyware attachment by sending it from an e-mail address just one character off from that of one of her friends. Pretending to be her friend, his e-mail contained spyware in an attachment named "for our soldiers.exe" (Mapes, 2007). When the victim opened the file, the spyware software installed itself onto her computer without any notification.

From 2002-2003, a commercial product called LoverSpy was purchased by more than 1,000 people and installed on more than 2,000 computers. It advertised that for $89 users could "monitor and record the complete computer activity of a computer user." Buyers could choose from a variety of seemingly innocuous e-greeting cards with built-in spyware software. When the recipient opened the e-card, the spyware installed itself and reported data back to the stalker (Magnus, 2005). In 2003, the LoverSpy operation was dismantled by the FBI, and in 2005, the creator of LoverSpy and four users were indicted on federal charges for illegally breaking into computers and intercepting the electronic communications of others (U.S. Department of Justice, 2005).

In a case in New York, a stalker illegally used spyware to gather information from the victim's computer at the medical office where she worked. He then called her patients claiming that the victim had disclosed their private medical information to him at a party. He also created an online blog in the victim's name with information about the patients and e-mailed the link to her employers (Cook, 2006).

Stalkers using spyware have been charged with a range of criminal offenses including unlawful interception of electronic communications and using a computer to commit a crime. In 2001, Steven Paul Brown of Michigan used spyware to spy on his estranged wife; he was charged with felony counts of eavesdropping, installing an eavesdropping device, unauthorized access, and using a computer to commit a crime (Granholm, 2003). In 2007, Shawn Macleod of Texas installed a spyware program on his ex-wife's computer to monitor her e-mails and the Web sites she visited. He was charged with unlawful interception of electronic communication, a second-degree felony that can carry a 20-year sentence. He was ultimately sentenced to four years in prison (Plohetski, 2007).

Stalking Using the Internet

In addition to using technology to monitor and track victims, stalkers are using the Internet to gather information about their victims, post damaging information about victims, and even impersonate victims. The Internet provides perceived anonymity for stalkers to brazenly harass victims, although a digital trail can almost always lead back to the stalker.

The volume of online data available to the public, and therefore to stalkers, is enormous. For victims, it is a constant challenge to manage the information posted online about them by government, information brokers, employers, family and friends, and even themselves. For stalkers, the plethora of data is a treasure trove of information they can use to track and harass their victims. One in four victims of electronic stalking reported knowing that their stalker used the Internet (blogs, Web sites, chat rooms, etc.) to stalk them (Baum et al., 2009).

Victims should be vigilant in monitoring information posted online about them since information can be posted by government agencies, employers, information brokers, and others. However, courts can help to ensure that a victim's privacy is respected, and records are not published to the Internet, whether by sealing records and/or giving the victim a pseudonym in the court docket. Stalkers should also be held accountable when they post false, misleading, or dangerous information about the victim online.

In the context of intimate partner violence, stalkers often harass their victims out of revenge, retaliation, spite, or anger. Various online services cater specifically to jilted or spurned lovers; these "revenge" Web sites encourage individuals to humiliate their ex by posting damaging information or photos. Getrevengeonyourex.com advertises itself as the ultimate revenge: "You can say what you like with absolutely no restrictions whatsoever! Using our secure, offshore and untraceable location, you can be safe in the knowledge that you can expose even the most personal of details" (www.getrevengeonyourex.com, 2010).

Some stalkers will post personal details about their victims, including personal health issues, sexual orientation, credit history, Social Security number, bank and mortgage information, driver's license photos, and more. Stalkers have even written or posted videos about what they will do to their victims. One stalker posted a video of himself on YouTube that showed him waving a handgun, threatening to shoot his ex-girlfriend and stating he was going to "put her face in the dirt until she can't breathe no more" (Malan, 2009). In this case, the victim got a protection order against the stalker, even though they were living in different states.

In addition to posting personal and damaging information about victims online, some stalkers will impersonate the victim by breaking into her e-mail or social network accounts (such as Facebook, MySpace, LinkedIn, etc.) and, pretending to be the victim, send out negative e-mails to the victim's friends, family, and colleagues or post false updates. Stalkers use the information they have gathered to wreak havoc on a victim's life: they can impersonate the victim in conversations with utility companies to have the power shut off, with attorney's offices to cancel appointments, or with the post office to reroute the victim's mail.

Impersonation is even easier when stalkers use technologies, such as e-mail, TTYs (telecommunication devices for the deaf and hard-of-hearing) and the Internet, where identities of senders cannot be verified. Stalkers have created e-mail accounts using the victim's personal information and name or hacked into social networking accounts and changed passwords so that a victim can no longer access her own accounts.

In one case, a police officer "seeking revenge against a former girlfriend, hacked into her e-mail account, assumed her identity at an online dating service, and contacted 70

men, inviting some of them for rendezvous at the woman's home" (German, 2006). In another case, an ex-boyfriend was accused of creating a post on craigslist.com and, pretending to be his ex-girlfriend, invited a "real aggressive man with no concern for women" to come to her home and rape her. One man responded to the ad and arranged a consensual forced sex arrangement, thinking that he was e-mailing the victim; in reality, he was communicating with the stalker. The stalker provided the victim's name, address, and even information on how to get into her home. Neither the man who responded to the ad nor the victim was aware that the entire event was orchestrated by her ex-boyfriend until after she was raped. Both men were charged with multiple felonies (Correll, 2010).

Situations like these are extreme but unfortunately are not entirely uncommon. In 2009, a North Carolina man was accused of arranging his wife's rape through craigslist-.com (Associated Press, 2009). In such situations, once the victim, her advocate, or law enforcement discovers where the information is posted, either law enforcement or an attorney can contact the Web site host.[2] Although some Web site hosts comply quickly and easily with takedown requests, other sites require notarized documents or police reports. Additionally, the victim may need help changing her phone number or finding a safe place to stay until she's certain that the post has been removed.

Impersonating a victim, spreading rumors about a victim, or convincing others to harm the victim are old tactics. Before the Internet, stalkers and abusers did it by word of mouth or social engineering. The Internet, however, expanded this traditional stalking tactic by giving the stalker more tools and a wider audience, which makes it more dangerous for victims. Nevertheless, the Internet also provides law enforcement with a digital evidence trail, as they can subpoena Internet service provider records and Web site logs as evidence of these crimes.

RESPONDING TO TECHNOLOGICAL MISUSE

When technology is being misused, investigators may have a very short window to collect the evidence. Text messages, for example, will stay on a mobile device for only a limited time. As more text messages come in, older messages are deleted. Furthermore, wireless carriers have varying policies on retaining customers' text message records. Some keep them for weeks, while other carriers will only keep days' worth of customers' text messages. Web site posts, on the other hand, may stay online until the owner of the site, whoever posted the information, or the Internet service provider takes them down. Even after that, archived or cached versions of the Web page may remain online and can still be searchable. Investigators should be aware of the time issue in digital evidence retrieval, such as text messages, voice mails, and Internet user records, because carriers may retain information for a limited amount of time.

Law enforcement and prosecutors should consider all state and federal laws that could apply to a case. If certain conduct does not fit the criteria of stalking, eavesdropping

2 Contact information for most Web site hosts and a variety of other technology service providers can be found at www.search.org.

or computer crime laws may apply. In the U.S., almost all computer crimes can be charged as federal crimes, since computer traffic crosses state lines by travelling through servers in different states.

When protection or restraining orders are issued,[3] judges can specify the type of contact that is prohibited. For example, even if the order already prohibits electronic contact, the prohibition may also specify that the stalker not access computers or phones used by the victim or contact the victim through e-mail or social networking services. The protection order can include a clause that prohibits the stalker from impersonating the victim online or from posting personal information pertaining to the victim.

If a victim and offender are required to have contact, such as for visitation or custody situations, the professionals involved must consider what safeguards should accompany that mandate. If there is to be electronic communication between the offender and the children, for example, consider who's required to purchase the equipment, who owns it, and who's allowed to make changes to the equipment. Even if an offender is prohibited from installing spyware on a victim's phone, the offender may be able to install spyware on their child's cell phone, particularly if it is paid for by the offender.

Although most evidence can still be taken at face value, it is important to know that there are a variety of ways that stalkers can mask the evidence of their crimes. As noted above, spoofing services can allow stalkers to make it seem as if the victim is calling them in an attempt to discredit the victim's claims. Billing records may document discrepancies by showing that those calls did not come from the victim's phone. Likewise, e-mail is also an easy way to falsify evidence. If a stalker refuses to confess to sending harassing messages, an investigator can trace the e-mails using IP addresses to determine the e-mail's true sender.

STALKING AND INTIMATE PARTNER VIOLENCE

Despite a common perception that people are stalked by strangers, studies have consistently documented that in the majority of stalking cases, the victim and the stalker knew each other. In one study, nearly three-quarters of all victims knew the offender in some capacity: as a romantic partner, friend, roommate, neighbor, or coworker (Baum et al., 2009). In another, at least half of stalking victims had an intimate relationship with the stalker (Spitzberg, 2002).

Stalking in intimate partner relationships is unique from other types of stalking because the victim and the perpetrator know each other well. The stalker knows what will terrify the victim and how to increase the victim's fear. Likewise, the victim also knows that what may seem innocuous and random to others is very specific and targeted to her.

3 Research shows that restraining orders are violated approximately 40% of the time (Spitzberg, 2002). As stalking expert Mark Wynn stated in an interview with the Stalking Resource Center, "Overlooking the threat posed by protection order violations is unwise and dangerous. This is often a signal to law enforcement that something worse is about to happen. When offenders thumb their noses at the court, this is an indicator that you've got high lethality on your hands" (Stalking Resource Center, 2004). States such as Florida have added a provision to their stalking law in which a stalking charge will be increased to a felony charge if the stalker violates a protective order (Fla. Stat. § 784.048, 2004).

For example, one victim may find 20 phone calls a day to be harassment, but another victim may find a phone call at 3:00 p.m. every day is more terrifying because that time has significant meaning to the victim and perpetrator.

While it is not uncommon for an abuser to stalk before, during, and after a relationship, the stalking behavior commonly increases after a break-up (Tjaden & Thoennes, 1998). For victims of intimate partner violence, leaving the relationship is often the most dangerous phase in an abusive relationship (Bachman & Saltzman, 1995). When a victim tries to leave the relationship or prevent the stalking (such as disconnecting phone numbers or switching jobs), the perpetrator may escalate the stalking behavior in an attempt to regain control over the victim.

As Beatty, Hickey, and Sigmon (2002) write:

> Stalking is less about surveillance of victims than it is about contact with them. If stalkers only wished to view the objects of their obsession from afar, they would not pose a serious safety risk. Stalkers, by their very nature, want more. They want contact. They want a relationship with their victims. They want to be part of their victims' lives. And, if they cannot be a positive part of their victims' lives, they will settle for a negative connection to their victims. It is this mind set that not only makes them "stalkers," but also makes them dangerous. Thus, virtually all stalking cases involve behavior that seeks to make either direct or indirect contact with the victim (para. 2).

Understanding the relationship between the stalker and the victim is important. Intimate partner stalkers want control and power over the victim. Particularly after a break-up, stalking and harassment are strong indicators of the stalker's desire to further his control over the victim and the relationship. In one study, 70% of the stalking victims said the perpetrator began stalking them with the goal of retaliation, spite, anger, or control (Baum et al., 2009). Furthermore, when compared to stranger stalking, the average total length of time a victim is stalked doubled in intimate partner stalking cases: 26 months compared to 13 months (Tjaden & Thoennes, 1998).

Many victims do not know all of the ways they are being stalked; they just know that they are being stalked and they often know the stalker's identity. Victims often tell advocates things like: "I mentioned to my mother that I might go to California for a vacation. Two days later, I ran into him at the grocery store and he asked me about my California vacation plans. How did he know that?" They may add: "When we were together, he seemed to know everywhere I went. If I went to the mall that day, he'd ask me if I bought anything. Even though he didn't know I went shopping. Now that we're no longer together, he still knows where I go, who I talk to, what I say, and sometimes even what I'm wearing."

For those unfamiliar with the patterns of intimate partner stalking, the above example may seem minor. After all, no threats were made, and the ex-partner actually seems thoughtful, asking about the victim's day and vacation plans. However, when someone the victim doesn't know or doesn't want to know any longer has that level of detail about her life, it can be disturbing and scary. Furthermore, when the victim tries to cut off connections with the perpetrator, such as dropping mutual friends, changing phone numbers, or moving to another place, and the monitoring continues or escalates, that can be a strong sign of increased risk and danger.

Studies show that current or former intimate partner stalkers are more likely to be physically violent and emotionally controlling (both during and after the relationship) than acquaintance and stranger stalkers (Harmon, Rosner, & Owens 1998; Pathé & Mullen, 1997; Sheridan & Davies, 2001). In one study, 81% of female victims were physically assaulted by their partners/stalkers, and 31% were sexually assaulted by their partners/stalkers (Tjaden & Thoennes, 1998). Victims are justifiably terrified when current or former intimate partners exhibit stalking behaviors because they are the most dangerous, the most determined, and the most likely to murder the victim (Sheridan & Davies, 2001).

In 1990, California passed the first U.S. anti-stalking statute after the brutal murder of actress Rebecca Lynn Schaffer and several other high-profile cases. The rest of the nation quickly followed, and by the mid-1990s all 50 states and the District of Columbia had passed anti-stalking legislation. In 1996, the U.S. federal Interstate Stalking Law was enacted to prohibit stalkers from traveling across state, tribal, or international lines in pursuit of their victims with the intent to kill, injure, harass or place under surveillance another person with intent to kill, injure, harass, or intimidate, placing that person in reasonable fear of death or serious bodily injury or causing substantial emotional distress to that person (18 U.S.C. § 2261A).

Within the U.S. legal system, stalking is generally considered to be a pattern of actions "that would cause a reasonable person to feel fear" (Baum et al., 2009, p. 3). Although the language of stalking statutes varies from state to state, some states "require prosecutors to establish fear of death or serious bodily harm, while others require only that prosecutors establish that the victim suffered emotional distress" (Baum et al., 2009, p. 3).

KEEPING VICTIMS SAFE AND HOLDING STALKERS ACCOUNTABLE

The complex and myriad ways stalkers misuse technology can be overwhelming for the victim as well as for professionals in the legal and criminal justice systems. One of the biggest challenges victims consistently face is convincing professionals that they are being stalked. In some cases, a stalker's behavior is minimized and misconstrued as the temporary behavior of a jilted, jealous, or hurt ex-lover. In other cases, the victim may have no visible physical injuries or there may have been no overt threats of physical injury. Finally, many victims must endure the stalking and harassment until it reaches a certain level of threat or harm before it can be addressed by the justice system.

While law enforcement officers often feel that their hands are tied until the stalker commits an action that is clearly a chargeable offense, they can ensure that the victim knows that she is not to blame for the stalker's behavior or actions and they are taking the stalking seriously. Additionally, law enforcement can work with the victim and the victim's advocate to identify the evidence that is needed and to help document the necessary information. For example, many jurisdictions suggest that victims keep a stalking log to document each stalking incident. By noting the date, time, location,

means of contact, and witnesses, stalking logs make it easier for law enforcement and prosecutors to prove a pattern of suspicious, threatening, or harassing behavior. While the onus of holding the perpetrator accountable should never be placed on the victim's shoulders, involving the victim in decision making can be empowering for the victim and provide valuable evidence for the prosecutor.[4]

As the case progresses, it is important that professionals help victims navigate the system, and ensure that the focus of all efforts remains on the victim's needs and that the options suggested are feasible. For example, law enforcement might interview the abuser or seize both the stalker's and the victim's computers. What increased risks does this create for the victim? Does the victim use that computer to operate a business that is her primary means of income? If so, it may be possible to duplicate the hard-drive and return it quickly. Situations like these must be carefully analyzed to ensure that the victim's safety is not neglected in the push for offender accountability.

Misconceptions about what technology can or cannot do are a concern as well. Sometimes called the "CSI effect," both victims and professionals may overestimate what technology can do, believing that everything shown on television or in the movies is possible in real life. A stalker's use of technology is limited by what the technology can do. Professionals in the legal and criminal justice systems may need to consult with technology experts to determine the capabilities of current technology. Advocates should identify the police and prosecutor technology crime specialists. If there are no specialized officers, learn what professionals in the community are doing to address child pornography as they often have the technological expertise necessary. Advocates should meet with the appropriate people in the jurisdiction to learn how they collect and process digital evidence and what local policies and practices are in place.

When trying to assess how technology misuse by a stalker has occurred, it is best to consider how something is happening rather than focusing on what technology is being misused. For example, if the victim believes the stalker knows everywhere she goes, instead of jumping to the conclusion that there are hidden cameras in the home, ask questions such as: Does he know where you are in your home or just where you go? Does he know where you are in real-time or does it seem like he knows after you've been there? These types of questions will help determine if there are cameras in her home or if there's a GPS tracking device on her car.

Investigators need to remain open to all possibilities when the victim talks about events that may seem coincidental or innocuous. These minor occurrences may constitute a larger pattern of stalking and harassment. Investigators may need to document the different types of technology misuse or events in order to establish a pattern of stalking, even if the technology use alone does not violate the law. Multiple hang-up calls a day may seem like just an annoyance, but combined with being locked out of online accounts, friends receiving strange e-mails, and the stalker having access to private information about the victim, investigators can build a case for stalking or harassment.

4 Some victims use their cell phone cameras to take photos of physical evidence like notes left on the front porch or the license plate of the stalker's car pulling away. It's important for advocates to caution victims against video recording a stalking incident until they've spoken to an attorney about local laws regarding requirements for obtaining consent before video or audio recording a third party.

Although stalkers use technology to stalk their victims, they have not stopped using traditional stalking methods. For example, if a victim believes the stalker knows everywhere she goes, whether she takes the bus, drives her own car or has her cell phone with her, the stalker may be using a network of friends to follow or keep tabs on her. Stalkers can be charming, and they often excel at getting information from others or coercing others to assist them in their stalking.

Some have suggested that the victim should simply stop using technology. However, ceasing use of a cell phone or a computer should never be a primary recommendation to any stalking victim. It is critical to remember that the technology is not the problem, the stalker's misuse of it is. Even if the victim were to stop using the technology, a determined stalker would quickly find other means to harass, monitor, and stalk. In fact, for some victims, changing phone numbers or blocking the abuser from e-mailing may actually increase the risk for violence. Because stalking of intimate partners is about power and control, any action that cuts the stalker's control may increase the risk of physical violence for the victim. In addition, some victims, such as people with disabilities, use technology to assist with activities and communication in their daily lives. It may be impossible for these victims to stop using the technologies that the stalker is misusing.

While stalkers are increasingly using technology to cause harm, the very tools they use also provide valuable evidence that helps lead to criminal convictions. Historically, stalking and abuse have had few witnesses beyond the victim. Technology has changed that, allowing investigators to retrieve a plethora of digital evidence against the stalker. From IP addresses to Internet browser histories to GPS logs, technology increases the ability to effectively hold stalkers accountable while also providing safety and justice for victims. Today, stalking is rarely committed with solely traditional or solely technological tools; most often, stalkers use a combination. As professionals find ways to reconfigure traditional investigation, prosecution, and advocacy strategies to fit this hybrid of physical and technological stalking, their new strategies must be flexible. After all, as technology continues to develop and stalkers adapt to these changes, the response of professionals will need to change as well to ensure that communities are equipped to respond to these crimes.

REFERENCES

Associated Press. (2009, June 4). Man accused of arranging wife's rape on Craigslist jailed on $200G bond. *Foxnews.com*. Retrieved May 13, 2010, from http://www.foxnews.com/story/0,2933,525097,00.html.

Bachman, R., & Saltzman, L. (1995). Violence against women: Estimates from the redesigned survey. *Bureau of Justice Statistics Special Report,* 1. Washington, DC: U.S. Department of Justice, Office of Justice Programs.

Baker, P., & Shane, S. (2010, May 5). Suspect was tracked through phone numbers. *The New York Times*. Retrieved May 11, 2010, from http://www.nytimes.com/2010/05/06/us/06cellphone.html.

Baum, K., Catalano, S., Rand, M., & Rose, K. (2009, January). Stalking Victimization in the United States. *Bureau of Justice Statistics Special Report*. NCJ 224527, 1-15. Washington, DC: U.S. Department of Justice, Office of Justice Programs.

BBC News. (2003, March 20). Text message stalker jailed. *BBC News.com*. Retrieved March 18, 2010, from http://news.bbc.co.uk/2/hi/uk_news/england/london/3043743.stm.

Beatty, D., Hickey, E., & Sigmon, J. (2002). Stalking. In Anne Seymour, Morna Murray, Jane Sigmon, Melissa Hook, Christine Edmunds, Mario Gaboury, & Grace Coleman (Eds.), *National Victim Assistance Academy Textbook*. Retrieved from: http://www.ojp.usdoj.gov/ovc/assist/nvaa2002/chapter22_2.html.

Boghossian, N. (2004, September 4). High-tech tale of stalking in the 21st century. *Los Angeles Daily News*, N1.

Cook, S. (2006, April 15). Police say man stalked wife via Internet, Court papers say suspect tapped into wireless signals. *The Daily Gazette*, (Schenectady, NY), A1.

Correll, D. (2010, January 11). Former boyfriend used Craigslist to arrange woman's rape, police say. *Los Angeles Times*. Retrieved May 11, 2010, from http://articles.latimes.com/2010/jan/11/nation/la-na-rape-craigslist11-2010jan11.

CTIA The Wireless Association. (n.d.) *Wireless Quick Facts*. Retrieved March 18, 2010, from http://www.ctia.org/advocacy/research/index.cfm/AID/10323.

Donovan, F., & Bernier, K. (2009). *Cyber Crime Fighters*. Indianapolis, IN: Pearson Education.

German, E. (2006, April 4). Officer charged with cyber-stalking his ex. *Los Angeles Times*, A19.

Getrevengeonyourex.com. (2010). Retrieved March 18, 2010, from http://www.getrevengeonyourex.com/v2/main/how-to-get-revenge/revengewebsite.php.

Granholm, J. (2003). *Biennial Report of the State of Michigan for the Biennial Period Ending December 31, 2002*. Retrieved August 20, 2010, from http://www.michigan.gov/ag/0,1607,7-164-34739_17343_25038---,00.html.

Harmon, R. B., Rosner, R., & Owens, H. (1998). Sex and violence in a forensic population of obsessional harassers. *Psychology, Public Policy and Law* (4), 236-249.

Jansen, W., & Ayers, R. (2007, May). Guidelines on cell phone forensics: Recommendations of the National Institute of Standards and Technology. *National Institute of Standards and Technology Special Publication 800-101*. Retrieved May 11, 2010, from http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf.

Jordan, A. (2010, February 5). The rise of caller ID spoofing. *The Wall Street Journal Blogs*. Retrieved March 18, 2010, from http://blogs.wsj.com/digits/2010/02/05/the-rise-of-caller-id-spoofing/.

Magnus, G. (2005, August 26). Five indicted over e-mail spyware program. *San Diego Union Tribune*. Retrieved March 18, 2010, from: http://www.signonsandiego.com/news/metro/20050826-1346-bn26spyware.html.

Malan, D. (2009, January 6). Threatening video leads to restraining order. *Connecticut Law Tribune*. Retrieved March 18, 2010, from http://www.ctlawtribune.com/getarticle.aspx?id=32469.

Mapes, A. (2007, June 11). Ex accuses officer of computer spying. *Fort Wayne Journal Gazette*. Retrieved March 18, 2010, from http://www.journalgazette.net/apps/pbcs.dll/article?AID=/20070609/LOCAL/706090348.

Miller, M. (2003, August 19). Man gets probation on wiretap conviction. *The Patriot-News*, B1.

Ohlson, K. (2003, October 6). Somebody's watching you. *Salon.com*. Retrieved March 18, 2010, from http://www.salon.com/life/feature/2003/10/06/stalking/print.html.

Pathé, M., & Mullen, P. E. (1997). The impact of stalkers on their victims. *British Journal of Psychiatry*, *170*, 12-17.

Plohetski, T. (2007, November 13). Spying on wife's email puts Austin man in prison. *Austin-American Statesman*, A01.

Rainie, L. (2010, January 5). *Internet, broadband, and cell phone statistics*. Washington, DC: Pew Internet & American Life Project.

Selfdestruct.com. (2010). Retrieved March 18, 2010, from http://www.sdmessage.com.

Sheridan, L., & Davies, G. M. (2001). Violence and the prior victim-stalker relationship. *Criminal Behaviour and Mental Health*, *11*(2), 102-116.

Smith, G. (2009, March 14). Alleged stalker uses text messages in campaign to harass and frighten victim. *The Post and Courier.com*. Retrieved March 18, 2010, from http://www.postandcourier.com/news/2009/mar/14/terror_by_cell_phone75052/.

Spitzberg, B. H. (2002). The tactical topography of stalking victimization and management. *Trauma Violence Abuse*, *3*(4), 261.

Stalking Resource Center. (2004). Protective Order Violations—Stalking in Disguise? *The Source*(4), 2. Retrieved March 18, 2010, from www.ncvc.org/SRC/main.aspx?dbName=DocumentViewer...46622.

Tjaden, P., & Thoennes, N. (1998). *Stalking in America: Findings from the National Violence Against Women Survey*. (NCJ 169592). Washington, DC: National Institute of Justice and Centers for Disease Control and Prevention. Retrieved from http://www.ncjrs.gov/pdffiles/169592.pdf.

Truth in Caller ID Act, H.R., 1258, 111th Cong., 2nd Sess. (2010).

Truth in Caller ID Act, S. 30, 111th Cong., 2nd Sess. (2010).

U.S. Department of Justice. (2005, August 26). *Creator and four users of Loverspy spyware program indicted. News Release Summary*. Retrieved May 13, 2010, from http://www.justice.gov/criminal/cybercrime/perezIndict.htm.