
A High-Tech Twist on Abuse: Technology, Intimate Partner Stalking, and Advocacy

Cindy Southworth, Safety Net Project at the National Network to End Domestic Violence Fund

Shawndell Dawson, Safety Net Project at the National Network to End Domestic Violence Fund

Cynthia Fraser, Safety Net Project at the National Network to End Domestic Violence Fund

Sarah Tucker, Safety Net Project at the National Network to End Domestic Violence Fund

authors commissioned by



Violence Against Women
Online Resources

Copyright © 2005 Violence Against Women Online Resources

June, 2005

Table of Contents

Acknowledgements	2
Introduction	2
Research and Scope	3
The Use of Technology to Stalk	5
Telephone Technologies	5
Location & Surveillance Technologies	6
Computer & Internet Technology	7
Advocacy Response: What Can Advocates Do?	8
Survivor Advocacy	8
Technology and Organizational Change	10
Technology & Legal Advocacy	10
Conclusion	11
Appendix A: Technology Safety Planning - Tips for Advocates	12
Appendix B: Annotated Resource Lists For Advocates	14
Appendix C: A Handout For Survivors	17
Technology Safety Planning with Survivors	18
References	19

Acknowledgements

The Safety Net Team wishes to thank and acknowledge assistance with this paper from Beth Zagorski, Pam Shea, the Stalking Resource Center at the National Center for Victims of Crime, and the many advocates that helped birth this paper and support survivors every day.

Introduction

"The information superhighway world we live in is a two-edge [sic] sword for survivors. The whole goal of escaping an abuser is to do just that, escape. After one has gone through the trauma of leaving, often with small children in tow, how horrifying it is to wake up to the reality that you can't escape at all. The Internet doesn't hide anyone." ---Survivor in Texas

Intimate partner stalking is not a new phenomenon. However, the ongoing advancement of technology is providing stalkers with a sophisticated selection of tools. Stalkers are using a variety of telephone, surveillance, and computer technologies to monitor and harass current and former intimate partners. Some abusers install global positioning systems to discover their victim's real-time location with extraordinary accuracy, while others use telephones to leave hundreds of messages in a single day. Still others use online databases, electronic records, and web search engines to locate, track, and harass former partners. While stalkers' methods and choice of technologies vary, survivors report that they are experiencing stalking and abuse that is perpetrated with a high-tech twist.

This paper presents information regarding new methods used to stalk, important safety planning tips, and action steps for local programs working to end violence against women. Advocates are encouraged to learn about these new stalking methods, expand traditional approaches to safety planning, and enhance the community response to victims of intimate partner stalking. The tips presented are not meant to read as a universally prescribed course of action. This paper offers many safety planning strategies, however the safest course of action may vary in each individual situation. Though many survivors of stalking are creatively using technology to increase their safety, this paper focuses on perpetrators' use of emerging and existing technologies.

Terms in this paper convey new ideas that build on existing knowledge of violence against women and stalking. Since people surviving abuse identify themselves differently, the terms "victim" and "survivor" are used interchangeably. "Stalker," "abuser," and "offender" are also used interchangeably to reference perpetrators of intimate partner violence -- a category encompassing domestic violence, sexual violence, and stalking that targets a current or former spouse, boyfriend, girlfriend, or significant other (Greenfeld et al., 1998).

Research and Scope

Only in the past 15 years has the legal system begun to recognize and address the crime of stalking. California passed the nation's first anti-stalking state law in 1990, following the highly publicized stalking and murder of actress Rebecca Schaeffer by a fan, and the much less publicized stalking and murder of five Orange County women by former intimate partners (Gilligan, 1992 as cited in Jenson, 1996). Over the next decade, anti-stalking laws were passed in all 50 states, the District of Columbia, and at the federal level (Stalking Resource Center, 2003). Despite some variation, these laws helped frame a general definition of stalking as "a course of conduct directed at a specific person that would cause a reasonable person fear" (National Center for Victims of Crime, 2004, p. 1).

The National Violence Against Women Survey (NVAW) begins to document the prevalence of stalking crimes by reporting that 1.4 million people are stalked annually and, by conservative estimates, at least 1 in 12 women and 1 in 45 men has been stalked at some point in their lives. Over three quarters (78%) of stalking victims are female and most (87%) stalking perpetrators are male (Tjaden & Thoennes, 1998).

Research indicates a clear link between stalking and intimate partner violence. Nationally studies show that former husbands, boyfriends, or cohabitating partners perpetrate a majority (62%) of the stalking incidents against females (Department of Justice, 2001). Of women stalked by current or former partners, eighty-one percent were physically assaulted and 31% were sexually assaulted by that same partner (Department of Justice, 2001). Stalking is also interconnected with the risk of being murdered by an intimate; in one review of women killed by intimate partners, 76% of the murders were preceded by one or more incidents of stalking (McFarlane, et al., 1999). Experts have even argued that "If stalking is defined as a course of conduct that intimidates or frightens the victim, then relationships involving domestic violence also involve stalking" (National Center for Victims of Crime, 2004, p.2).

New forms of technology and increased access to technology provide stalkers with new tools to terrorize current or former intimate partners. "The information revolution has vastly increased the scope of technologies of intrusion" and thus "expanded the arsenal of the stalker" (Spitzberg & Hoobler, 2002, p.72). As of late 2003, 63% of adult Americans were using the Internet (Madden & Rainie, 2003). As of December 2002, about 102 million Americans were email users (Madden & Rainie, 2003). While it is difficult to determine the prevalence of technology use by intimate partner stalkers, qualitative evidence -- testimony from survivors and highlights from representative research studies, convenience samples, and anecdotal cases -- indicates an urgent need to address safety risks for victims while concurrently assessing the extent and prevalence of technology misuse.

Awareness of technology harassment began in the mid-1990s, when Internet users began reporting online harassment and threats. This use of technology was labeled "cyberstalking". A 1999 U.S. Congressional Report defines cyberstalking as "the use of the Internet, e-mail, or other electronic communications devices to stalk another person" (Department of Justice, 1999, What Is Cyberstalking section, para 1). Others have defined cyberstalking more broadly to include the use of electronic communication including pagers, cell phones, emails and the Internet, to bully, threaten, harass, and intimidate a victim (Laughren, 2000; Ellison & Akdeniz, 1998; CyberAngels, 1999; Dean, 2000; Ogilvie, 2000; Maxwell, 2001). A 1998 study noted, "electronic stalking often leads to, or is accompanied by, physical stalking, and explicitly or implicitly threatens physical stalking" (Lee, 1998, p. 391). To recognize the full range of technologies, stalking experts are moving away from the term "cyberstalking" and beginning to use "the use of technology in stalking" (Bahm, 2003, p.2).

While there are no comprehensive studies, several reports document specific technology types used by stalkers. In particular, certain studies have recorded the use of telephones, email, and instant messaging in stalking. For example, in a survey of women stalked by former intimate partners, over 90% reported telephone calls from their stalker (Brewster, 2003). A national study of stalking victims found that females (62%) were significantly more likely than males (42%) to receive repeated unwanted telephone calls from their stalker (Finn, 2004). Unfortunately, data is limited, and the few studies that record telephone use in stalking do not report information about the type of telephones (e.g. cell, cordless), telephone-related technologies (e.g. pagers) or integrated location and surveillance devices (e.g. cameras, global positioning systems).

Popular culture often focuses on cyberstalking via email and instant messaging and some studies document these methods of stalking. As early as 1997, a nationally representative study of students attending 223 U.S. colleges and universities reported that 13.1% of female students were stalked during the first seven months of the 1996-1997 school year; nearly 25% of these victims reported being stalked via email (Fisher, Cullen, & Turner, 2000). At least 20% of the cases reported in a 1999 survey of criminal justice and investigation units involved email or electronic communications and electronic harassment or threats (Department of Justice, 1999). The organization Working to Halt Online Abuse (WHOA) discovered that 58% of the people who contacted them for support in 2003 knew their harasser previously, and 57% of the harassers were former partners (WHOA, 2003). In a recent randomized, convenience sample of University of New Hampshire undergraduate students, 9.6% of students surveyed reported receiving threats, insults, or harassment from significant others via email, and 11% received threats through instant messages (Finn, 2004).

To date, there are no nationally representative studies that explore the breadth of information, communications, and surveillance technologies being used in intimate partner stalking. Additional research is needed to examine the extent to which various technologies are being used to stalk victims of intimate partner violence. Survivors would greatly benefit if future violence against women research addressed the context and use of specific technologies in intimate partner violence and stalking. Additional qualitative research would enhance survivor safety by identifying appropriate and useful system and community responses.

Stalkers use numerous technology and non-technology tools to stalk, monitor, and intimidate their victims. Advocates must learn about and address these high-tech tactics, but always in the larger context of a victim's stalking experience. As Tracy Bahm, the Director of the Stalking Resource Center in Washington, D.C. states, "No matter what tools they use, stalkers are still stalkers" (Bahm, 2003, p.2).

The Use of Technology to Stalk

Survivors report that stalkers are using many forms of technology - old and new - to control, coerce, and intimidate them during and after relationships. Some stalkers inundate former intimate partners with "dozens of emails and instant messages, often using automated senders and anonymous remailers that make it hard to identify the source" (Lamberg, 2001, Cyberstalking: A Growing Threat section, para 2). Other stalkers use technologies such as caller ID during a relationship to monitor their partner's calls, and to locate her after she has fled.

This paper includes highlights of some of the common abuses of technology, including a sampling of survivor stories collected by Safety Net: the National Safe and Strategic Technology Project at 191 training sessions to over 10,000 advocates, law enforcement officers, and allies. This section begins with telephone technologies, continues with global positioning systems, hidden cameras, computer monitoring devices, and ends with online databases. Advocacy tips are also included to provide options for addressing survivor safety issues. As existing technologies are changing and new technologies are emerging, these strategies provide an adaptable starting point for advocates to include technology in current safety planning efforts.

Telephone Technologies

Abusers regularly use telephone technologies to stalk current and former intimate partners (Brewster, 2003). While most homes have traditional telephones, many families are also using cellular and wireless telephones, creating a new realm of tools for stalkers to use. In June 2004, approximately 169 million Americans used wireless telephones (Cellular Telecommunications & Internet Association, 2004). As wireless telephones become more sophisticated, abusers are finding ways to use advanced telephone features to aid them in stalking their victims. However, abusers have also found creative ways to stalk with even the most basic telephone technologies.

Telephones. Abusers commonly stalk through repeated and harassing telephone calls, sometimes using prepaid calling cards or prepaid cell phones that leave minimal information trails. If a phone card is not activated with a credit card, linked to a discount card, or billed to a person's long distance

phone carrier, the harassing call can be difficult to trace. Perpetrators also leave threatening messages in voicemail and on answering machines.

Caller ID. Caller Identification (Caller ID) is a popular tool that abusers may use to monitor their victim's telephone calls while in the relationship, and to stalk and locate their victim after the relationship has ended. Caller ID devices provide the name and number of the caller, and some even provide the address of the caller. In 1995, soon after caller ID was first available, an abuser tracked down and subsequently murdered his former girlfriend by using caller ID (Associated Press, 1995).

Fax Machines. Abusers and stalkers have used the fax header on faxed documents to locate their victims. New fax machines also contain caller ID, creating additional safety challenges for survivors. In one example, a woman fled, but had to send papers to her abusive partner. She faxed the papers from the shelter fax machine to her attorney. Her attorney faxed the papers to his attorney. His attorney gave the papers to him. Since no one removed the fax header, the abuser acquired the telephone number and location of his victim and she had to relocate again (Safety Net, 2004).

TTY/TTD. Teletypewriters (TTY) and Telecommunications Devices for the Deaf (TTD) are text based telephones that people who are deaf or hard of hearing use to communicate. These devices often record and save an exact history of conversations, making it easier for stalkers to monitor victims' conversations. Abusers also impersonate victims by using their TTY to seek information about her activities. In one case, a prosecutor working with a Deaf victim got a call on his TTY, allegedly from the victim, reading, "If you don't drop the charges against my boyfriend, I'm going to kill myself." When help was sent to the victim's home it was found that she had been sleeping when the TTY call was made. The abuser had impersonated the victim in an attempt to persuade the prosecutor to withdraw charges (Safety Net, 2004).

Cellular & Wireless Telephones. Abusers can monitor their victims' cell or wireless telephone use through the call history on the telephone and through billing records. Most cell phones keep an internal record of incoming and outgoing calls. Stalkers also use phone-based instant messaging, simple text messaging, and pagers to maintain constant access to their intimate partners. Stalkers can use new location based services provided by cell phone carriers to track the location of their victims. In Rhode Island one abuser assaulted his wife after finding the shelter telephone number in her cell phone call history; as a result she did not attempt to leave her husband for another year (Safety Net, 2004).

Location & Surveillance Technologies

Stalkers are increasingly using basic and sophisticated location and imaging technology to conduct surveillance, thus putting victims' safety at great risk. Before abusers had access to location tracking devices like global positioning systems, they often checked car odometers to measure mileage and monitor victims' daily activities. Now, tools ranging from inexpensive digital cameras to high-tech streaming video cameras and global positioning systems, while not inherently surveillance devices, are being used as such by perpetrators.

Global Positioning Systems. Abusers use Global Positioning Systems (GPS) that use satellite receivers to provide precise real-time worldwide positioning, to locate and follow victims. These

devices vary by price, size, and appearance. GPS may appear as a small black box, a hand-held unit, or even a small chip in a wristband. Global positioning technology can also be part of anti-theft services for vehicles such as OnStar. In December 2002, a Wisconsin man secretly installed a GPS device under the hood of his ex-girlfriend's car and stalked her for months. "He would follow her as she drove to work or ran errands. He would inexplicably pull up next to her at stoplights and once tried to run her off the highway" (Orland, 2003, para 2). Since GPS devices are becoming cheaper and smaller as technology advances, it is imperative that survivors are educated about the ways to check for such devices.

Hidden Cameras. Stalkers use small hidden cameras to monitor their victims and learn their routines. Stalkers use information they gather to exert power and control over their victims. Small wireless high-resolution cameras can be hidden in smoke detectors, children's lamps, or behind a pin-sized hole in a wall, and can even be activated remotely. In 2003, the Supreme Court of New Jersey found that a defendant's video surveillance of his estranged wife in her bedroom presented a prima facie case of stalking and harassment under the New Jersey Domestic Violence Act (H.E.S. v. J.C.S., 2003).

Computer & Internet Technology

Abusers continue to identify and adapt new computer software and hardware tools that allow them to further stalk and harass their victims. They not only use low-technology monitoring options such as viewing the website browser history or intercepting email, but also are increasingly using more sophisticated SpyWare software and hardware for surveillance. A study of students at the University of New Hampshire found that approximately 10 - 15% of surveyed students reported receiving threatening or harassing email or Instant Messages (Finn, 2004).

Computer Monitoring Software. Computer Monitoring Software, or "SpyWare", was originally developed to monitor children's Internet use, but has also been utilized by abusers. It allows an abuser to monitor computer and Internet activities and discover a victim's efforts to escape or access help. This software can be installed remotely or by physically accessing the victim's computer. Although SpyWare detection programs claim to uncover the hidden SpyWare programs, they are imperfect in their counter surveillance. "Scrubber" and "Washer" programs that claim to clear computer histories are ineffective if SpyWare is in use. Additionally, if the victim installs new programs or clears all computer trails, this could cause suspicion and increase danger. In September 2001, a Michigan man was charged with installing spy software on the computer of his estranged wife. Without her knowledge, a SpyWare program sent him regular emails reporting all of her computer activity, including all emails sent and received and all web sites visited (Wendland, 2001).

Keystroke Logging Hardware. In addition to software programs, stalkers can use hardware devices called "Keystroke Loggers" that are inserted between the keyboard cable and the back of the computer. These tiny devices contain small hard drives that record every key typed, including all passwords, personal identification numbers (PIN), websites, and email. Abusers with physical access to a victim's computer can install and check these hidden devices. SpyWare software detection programs cannot detect hardware loggers. Both SpyWare software and keystroke logging hardware are advertised as products allowing one to easily "spy on your spouse."

Email & Instant Messages. Abusers are using email and instant messages to threaten victims and impersonate them. Stalkers can send victims malicious SpyWare or viruses as email attachments. Abusers are monitoring email and impersonating victims by stealing passwords and viewing email via SpyWare. One abuser changed his wife's email password and sent threatening messages to himself from her email account. He then took the printed messages to the police and asked them to arrest her. Another abuser killed his wife after discovering that she was planning to flee. He learned of her escape plan in an email in her "deleted email folder". (SafetyNet, 2004).

Websites. Stalkers are setting up websites that threaten victims or encourage others to contact, harass, or harm the victim. Some abusers encourage others to stalk their victim by posting erroneous and harassing information on websites (e.g. that the stalker's ex-wife enjoys being raped). In one scenario, an abuser had his parental rights terminated when his child was a toddler. Years later he posted a very old family photograph and details about his then ten-year-old child. The mother and child were terrified to discover the presence and content of this website (Safety Net, 2004).

Online Databases and Information Brokers. Stalkers use free and fee-based websites to track private information about their victims. Information brokers are commercial entities that buy and sell data, and frequently acquire information from public records and retail databases. In addition to fee-based services, many free websites such as court databases, voter registration, and religious directories provide a wealth of private contact information that can be used to track survivors nationwide as they attempt to relocate. Many courts are beginning to publish both indexes of court records and the full documents and case files to the Internet, often without providing any notice to citizens or options for victims to restrict web-access. The Montgomery County, Pennsylvania Court went a step further, publishing the names and addresses of victims (and their children) who obtain protection orders on the Internet (Webster, 2003, December 1).

Advocacy Response: What Can Advocates Do?

Victims of abuse begin to plan for safety well before they reach out to advocates and other practitioners for assistance. It is vital that advocates continue to support the strategies survivors have been successfully using to help them navigate the abuse and stalking in their lives. Regardless of an advocate's own level of technological expertise, it is important that advocates work with survivors to plan for safety around technology and stalking. Although technology is changing rapidly and abusers are adept at misusing these new tools, advocates should remember that the motive for stalking is not affected by technological advancements. Abusers stalk in order to maintain power and control over a victim. Therefore, safety planning with survivors about technology methods used to stalk her may have a similar format to other non-technology related safety planning approaches and advocacy. (See appendixes for further resources and materials.)

Survivor Advocacy

Some survivors have found that disconnecting a telephone line or email account in an attempt to thwart a stalker results in the abuser escalating to a new method of control or access. Advocates can work with survivors to find ways to limit stalker access, collect evidence, and maintain their safety. For example, some survivors have installed a new telephone line, but left the old telephone

number connected with the ringer turned off. This allows them to document the continued harassing calls with an answering machine and caller ID. Advocates must work with victims to navigate these risks and weigh the potential safety risks of evidence collection. For example, law enforcement might interview the abuser or seize the stalker's computer. Advocates need to discuss with the victims the possible increased risks that law enforcement or criminal justice system involvement might create. Sometimes stalkers react violently when they find out that the victim has reported to the police or sought a protection order. These types of interventions are often necessary and life-saving, but victims need to know that stalkers are unpredictable and these interventions also may bring risk. Advocates need to safety plan with victims accordingly. Situations like these must be carefully analyzed to ensure that victim safety is not overlooked in an effort to hold offenders accountable.

Strategies for Advocates:

- Focus on the survivor's needs and make sure that the options suggested are feasible.
- Try to share information about technology safety risks in ways that are relevant to the concerns raised by a survivor. Some survivors may feel relieved to finally figure out why their stalkers are able to know everything they do; others may choose to focus first on other priorities and prefer to discuss technology information later.
- Consider introducing the topic of technology stalking and safety in survivor support groups. Also educate victims about the positive benefits of emerging technology tools that can enhance their safety.
- Educate survivors about these new tools and the potential use of technology to stalk without prohibiting access to technology. For example, explain cell phone features to survivors, but do not ban cell phones from shelter. Advocates might also provide safer computer and Internet access and education to victims in shelter.
- Some survivors may have heightened risks of stalking through technology and may need additional information and support. For example, some people with disabilities rely on assistive technologies to communicate and access resources online and might be more vulnerable to specific methods of technology monitoring and stalking. Consider additional factors -- such as geographic location, ethnicity, income, accessibility, age, or sexual orientation -- that could impact a survivor's access to or reliance on various communications or technology.
- Educate survivors about the timing challenges of some digital evidence such as voicemail messages, telephone traces, Internet user records, and email "headers." If a victim wants to report these crimes to the police, law enforcement may have a short window to collect the digital evidence since many companies only retain the information for a very limited amount of time. For example, some Internet service providers only keep user records for thirty days.

Technology and Organizational Change

There are many critical action steps advocates can implement within their organizations to improve the response to victims and increase survivor safety regarding technology. First, advocates can educate and train all staff and volunteers about both the positive benefits of technology and also how abusers are misusing technology to stalk their partners. Next, advocates should examine if high-tech stalkers could compromise any of their own organizational practices.

Many nonprofit organizations and government agencies are embracing technology without a thorough understanding of potential unintended consequences. As data systems become increasingly interconnected, it is vital that advocacy organizations anticipate and minimize the potential for harm to survivors, by securing the confidentiality of all communications, and reexamining and minimizing any data about survivors that is collected, stored, and shared. Additionally, since some victims will request online assistance or advocacy, it is critical for advocates to think proactively through all safety, confidentiality, stalking, and monitoring possibilities, and, to create survivor-centered organizational practices that increase confidentiality, informed consent, and safety planning (Finn, 2001; Kranz, 2001).

Strategies for Advocates:

- Revise organizational communication, records, and confidentiality policies to include technology security issues.
- Update organization website safety information for victims searching for support online. Also, ensure that your website is accessible to all survivors, including individuals with disabilities who use assistive technology such as screen readers.
- Create organizational policies that address how (or if) to respond to emails from victims. When reviewing policies, consider the possibility that abusers may be monitoring the victim's email account or computer, so policies should focus on how to increase safety and always provide informed consent.
- Increase victim safety by securing survivor data. Only store victim information on computers that are not connected to the Internet or networked to the Internet. If using an Internet-based database for victim records, designate a computer to use only for that purpose. To minimize hacking and SpyWare risks, do not store other victim files on that computer or use it for email or Internet browsing.
- Given that abusers work in every field and some are extremely skilled in using technology, evaluate data collection and sharing policies to keep victim data out of the hands of stalkers, abusers, and members of the public.

Technology & Legal Advocacy

As stalkers increase their use of technology, it is vital that communities are equipped to respond to these crimes. In an age where stalkers can easily use search engines to track them, victims need

to be able to relocate safely. As more records are published to the Internet, advocates must educate community agencies, courts, and government offices about the potential dangers to victims and the importance of notification and privacy options. When electronic evidence is needed to prosecute a crime, advocates can work to ensure that specialized violence against women law enforcement and prosecution units receive additional training or access to a technology crime unit. Whether working within the legal system, community social services, or with other civic organizations, education and systems advocacy are critical to lessening the barriers victims of technology stalking encounter.

Strategies for Advocates:

- Identify training opportunities on technology investigation, computer forensics, or prosecution, and attend these trainings with law enforcement or prosecutors from your community. Many states have computer crime units or prosecutor associations that may be available to support and train local jurisdictions.
- Identify the police and prosecutor technology crime specialists. If the community does not have a technology unit, identify officers and prosecutors with technology experience. Discuss how law enforcement process digital evidence and conduct investigations.
- Work with law enforcement to identify what evidence is needed, so advocates can work with survivors to document the necessary information. Encourage officers and survivors to discuss how the investigation will impact the victim's life. For example, if a victim's computer is seized, it may be possible to duplicate the hard-drive and return it quickly.
- Work with the legal system to identify the state laws that could apply to emerging technology strategies of stalkers. Some stalking laws only include electronic communication devices, so prosecutors may need to use eavesdropping or other statutes to address some crimes.
- Ask that prosecutors discuss the potential consequences with a survivor of pursuing a technology related criminal charge compared to a domestic violence or stalking charge, so that she remains informed of how potential media coverage and evidence collection practices might impact her life. For example, national and international media covered the Michigan SpyWare and the Wisconsin GPS stalking cases.
- Join community committees discussing Internet publication of court or voter records and advocate for privacy provisions for survivors.

Conclusion

While much is unknown about the future of technology and the emerging uses of technology in intimate partner stalking, advocates and allies must continue to press on - learning, educating, and advocating for change. Stalkers are persistent and resourceful, but so are the advocates and survivors working against them.

Advocates should educate survivors and colleagues about emerging stalking methods, expand safety planning to include technology, and work with their local community systems to address the use of technology in intimate partner stalking. While it is imperative to immediately begin addressing technology issues, it is also important to realize that as technology continues to develop and abusers adapt to these changes, the response of advocates must change as well.

Anecdotal and empirical evidence clearly indicate that traditional modes of stalking have expanded, but significant research is needed to fully understand the parameters and types of technology used in stalking. Research is also needed to document the myriad of ways in which victims are creatively using technology to enhance their safety. More thorough study and documentation of use of technology by intimate partner stalkers is needed to expand our understanding of what survivors are experiencing and to inform the systemic change needed to address this issue. In the interim, advocates and allies are vital resources in providing critical support and helping victims plan for safety.

Appendix A: Technology Safety Planning - Tips for Advocates

This checklist of tips for advocates is intended to accompany the attached paper.

Telephones:

- Talk to survivors about screening calls with answering machines and, where legal, taping harassing telephone calls.
- Encourage victims to document harassing calls through stalking logs, photographing caller ID, and "call trace" (*57 in most areas).
- Educate survivors about "per-call" (*67 in most areas) or permanent caller ID blocking.
- Inform victims that caller ID devices can be installed without their knowledge and transmit information about all incoming calls.
- When calling victims, use caller ID Block or operator-assisted calls to reduce the risk of an abuser identifying an advocacy organization through a caller ID device.
- Call ahead before sending any faxes on behalf of a survivor. Encourage victims to do the same when they are not in shelter. Remind the fax recipient to cut off the fax header and remove cover page.
- Block caller ID on shelter and advocacy organization fax and telephone lines.
- Encourage victims to use a password or phrase when using communicating by TTY to confirm their identity and minimize the risk of impersonation.
- Talk with victims about deleting TTY conversation histories stored in their TTY devices.

- Provide a TTY device in advocacy offices that victims can use to make private calls.
- Encourage survivors to contact their telephone carriers to learn about their wireless/cell phone's features and services. They may want to ask if location services have been added to their service plans.
- Educate survivors about the option of turning a phone off to increase location privacy. Educate and strategize, but do not prohibit the use of cell phones in shelters or advocacy offices.
- Encourage survivors to use a donated cell phone or to purchase a new cell phone with a different carrier if they think their phones or the billing records are being used to monitor their calls.

Location and Surveillance:

- Encourage victims to trust their instincts if they suspect they are being followed.
- Help survivors find a law enforcement officer or a mechanic willing to search a victim's car or belongings for a GPS device.
- Talk to victims who use GPS automobile services about the pros and cons of changing their account password to prevent stalkers from gaining access to their car and location information.
- Encourage survivors to trust their instincts and look for patterns in the information the stalker appears to know. Patterns may help the survivor identify possible camera locations.
- Talk to survivors about checking their homes or having law enforcement search for small holes or unidentifiable wiring.

Computers:

- Encourage victims to use a safer computer; one that the stalker does not have access to.
- Encourage survivors not to open any attachments from unknown sources or their abusers, and to keep their computers' operating systems and virus definitions updated regularly.
- Ask victims if they use a computer and, if so, explain how SpyWare can give an abuser the ability to monitor ALL computer use. Discuss the pros and cons of using SpyWare detection programs, since installing such a software program could alert the stalker.
- Encourage survivors to be suspicious if an abuser has installed a new keyboard recently or done computer repair work that coincides with an increase of stalking or monitoring.
- If a victim finds a harassing website about herself, discuss with her the option of talking to law enforcement to determine whether a website is a violation of a protection order or could be evidence for a stalking or harassment charge.

- Help victims use search engines such as www.whois.net to determine the owner of a malicious website and research the website owner's policy on threatening sites.
- Encourage victims to ask where their personal information is stored; if any government entities publish their records on the Internet, they can request to have their records sealed or to restrict who can access their information.
- Identify or promote approaches, such as address confidentiality programs, which provide viable mechanisms to ensure a victim's information remains confidential regardless of whether she votes, buys property, goes to court, or engages in other activities.

Appendix B: Annotated Resource Lists For Advocates

This list highlights select technical assistance projects, websites, and written materials chosen for practical usefulness to advocates who are working with survivors of technology-based intimate partner stalking.

A. U.S. Technical Assistance Projects

The Safety Net Project at the National Network to End Domestic Violence Fund 660 Pennsylvania Ave SE, Suite 303; Washington, DC 20003 Phone: 202-543-5566 x 22 Fax: 202-543-5626 Email: safetynet@nnev.org [<mailto:safetynet@nnev.org>]<http://www.nnev.org>**Description:** Launched in August 2002, Safety Net: the National Safe & Strategic Technology Project at the National Network to End Domestic Violence Fund (NNEVDV) addresses all forms of technology that benefit survivors, are misused by abusers, or impact survivors in their communities. The Safety Net Project provides training and technical assistance to U.S. state domestic violence coalitions, local advocates, law enforcement, prosecutors, and allies on all forms of technology that impact victims of abuse.

The Stalking Resource Center at the National Center for Victims of Crime 2000 M Street NW, Suite 480, Washington, D.C. 20036 TTY: 1-800-211-7996 Phone: 1-800-FYI-CALL (1-800-394-2255) Fax: 202-467-8701 <http://www.ncvc.org/src>**Description:** The Stalking Resource Center is a program of the National Center for Victims of Crime. Launched in July 2000 with funding from the Office on Violence Against Women, their dual mission is to raise national awareness of stalking and to encourage the development and implementation of multidisciplinary responses to stalking in local communities across the U.S. The Stalking Resource Center provides training and technical assistance on all forms of stalking (including high technology stalking) and community response. The Stalking Resource Center maintains a website with articles, news stories, stalking legislation and case law, and many more resources for practitioners and victims. In addition, they produce two newsletters per year and have brochures that can be downloaded from their website.

The National Domestic Violence Hotline /Linea Nacional sobre la Violencia Domestica PO Box 161810, Austin, TX 78716 TTY 1-800-787-3224 Phone: 1-800-799-SAFE (7233) <http://www.ndvh.org>**Description:** This toll free hotline enables victims of domestic violence, their families, advocates, and friends to call trained hotline advocates/counselors who will provide confidential

crisis intervention, support, information and referrals to local programs. The hotline links people to shelters, and legal and social assistance programs in their geographic area. Advocates provide help in English and Spanish with interpreters available for 139 languages. Crisis intervention and referrals are available to the Deaf through a TTY line or by email to deafhelp@ndvh.org [mailto:deafhelp@ndvh.org] Call the hotline 24 hours a day from anywhere in the U.S.

B. Websites on Responding to Technology Use in Intimate Partner Stalking

The Privacy Rights Clearinghouse<http://www.privacyrights.org>**Description:** The Privacy Rights Clearinghouse is a nonprofit consumer education, research, and advocacy program. While PRC's information is written for the general public and does not specifically focus on intimate partner stalking, advocates can find many fact sheets, speeches, and articles with overviews and practical tips for survivors on internet privacy, various telephone and telecommunications issues, public and government records, and more.

Stalking Resource Center - Stalking Laws & Court Cases collections Stalking Laws: http://www.ncvc.org/src/main.aspx?dbID=DB_All_Legislation188 Stalking Court Cases: http://www.ncvc.org/src/main.aspx?dbID=DB_All_Case_Law508**Description:** These web-based collections present laws and court case summaries for various U.S. jurisdictions: federal, federal interstate, state, and Tribal. These are useful for educating advocates and survivors about laws that can be used to hold an abuser accountable for using technology to stalk. The text of stalking laws and related legal offenses such as: harassment by telephone, cyberstalking, and unlawful computerized communications are covered in the stalking laws state-by-state section. The stalking court cases section summarizes federal and state court case findings, including where using technology to stalk an intimate partner was found by law to be a crime.

SafetyEd International<http://www.safetied.org>**Description:** Housed in New Zealand, this website provides education regarding online safety and privacy. It includes research articles, online workshops, U.S. legal summaries, and other advocacy articles on cyberstalking.

Working to Halt Online Abuse (WHOA)<http://www.haltabuse.org>**Description:** WHOA fights "online harassment through education of the general public, education of law enforcement personnel, and empowerment of victims". WHOA's website provides links to various resources regarding online harassment and stalking, and suggests some tips to increase safety. WHOA responds to a range of issues faced by survivors of stranger and acquaintance stalking, many of which can also be relevant to intimate partner stalking.

C. Written Materials on Responding to Technology Use in Intimate Partner Stalking

Address Confidentiality Programs**Author:** Vote Power Project, NNEDV Fund (2004) **Description:** This document lists U.S. states with address confidentiality programs, and provides telephone numbers and web-based access to relevant state forms, qualifying information, and process steps. <http://www.nnedv.org/projects/votepower.html> [<http://www.nnedvfund.org/default.asp?Page=63>]

Annotated Stalking Bibliography**Author:** Stalking Resource Center, National Center for Victims of Crime (NCVC) **Description:** This bibliography provides brief summaries of over thirty materials

on stalking, all published after 1994. The bibliography notes when the article addresses intimate partner stalking or cyberstalking. http://www.ncvc.org/src/main.aspx?dbID=DB_Annotated_Stalking_Bibliography344 [http://www.ncvc.org/src/main.aspx?dbID=DB_Annotated_Stalking_Bibliography344]

Data Security Checklist to Increase Victim Safety & Privacy **Author:** Safety Net: the National Safe & Strategic Technology Project, the National Network to End Domestic Violence Fund (Safety Net, NNEDV) (2004) **Description:** This handout provides steps to consider when undertaking such activities as designing a data collection system or securing a local organization's network. These tips help ensure victim-related data will be better protected and remain confidential from high-tech stalkers and hackers. http://www.nnedv.org/docs/SafetyNet/NNEDV_DataSecurity.pdf

Domestic Violence Organizations Online: Risks, Ethical Dilemmas, and Liability Issues **Author:** Jerry Finn (2001) **Description:** This paper outlines risk and liability considerations related to the use of the Internet for advocates working with survivors of stalking and domestic violence. It discusses potential safety, privacy, and security risks for survivors communicating and accessing direct services online. http://new.vawnet.org/category/Documents.php?docid=429&category_id=93

Helpful or Harmful? How Innovative Communication Technology Affects Survivors of Intimate Violence **Author:** Ann L. Kranz (2001) **Description:** This paper explores web usage by both survivors of intimate violence and the organizations that serve them. It highlights ways that batterers use communication technology to monitor and control their partner's activities, and notes safety and other precautions survivors and organizations can employ. <http://www.sexcriminals.com/library/doc-1050-1.pdf>

How Tracking Systems Place Victims at Risk: Homeless Management Information Systems & Victims of Abuse and Stalking **Author:** Safety Net, NNEDV (2004) **Description:** This handout discusses victim privacy concerns related to the collection, sharing, and storage of data, to ensure intimate partner stalkers cannot access data. It provides advocacy strategies to consider when community members want an organization to share identifiable victim data. The document focuses on the implementation of homeless databases in the U.S., but highlights safety concerns relevant to all victims of stalking and abuse. <http://www.cfp2004.org/program/materials/p1-southworth.pdf>

Protect Your Phone Privacy / Proteja su Privacidad Telefonica **Author:** Pennsylvania Coalition Against Domestic Violence (1998, in English and Spanish) **Description:** This handout for victims of domestic violence, harassment, and stalking notes U.S. options for blocking telephone calls using "caller ID", "line blocking", and "per call blocking". http://new.vawnet.org/Assoc_Files_VAWnet/CallBlok.pdf

Public & Internet Access to Court Records: Safety & Privacy Risks for Victims of Domestic Violence & All Citizens Using the Justice System **Author:** Safety Net, NNEDV (2003) **Description:** This document provides information regarding technology-stalking risks for victims and the importance of protecting victim privacy when court systems post partial or complete court records on the World Wide Web.

StalkingAuthor: National Center for Victims of Crime (In Problem-Oriented Guides for Police Problem-Specific Guides Series No. 22, 2004) **Description:** This guide covers the prevalence and nature of stalking, the impact of stalking on victims, and recognizes stalking as a pervasive tactic of those who perpetrate domestic violence. It mentions ways technology is used to stalk including: harassing telephone calls or emails, invasive computer monitoring programs, wiretapping, use of location devices and wireless remote cameras, and identity theft. The guide notes challenges to policing stalking and recommends responses to stalking, including practical suggestions for police around investigation. <http://www.cops.usdoj.gov/mime/open.pdf?item=1042>

A Study on Cyberstalking: Understanding Investigative HurdlesAuthor: Robert D'Ovidio & James Doyle (In FBI Law Enforcement Bulletin, March 2003, 10-17) **Description:** This article summarizes the technological methods used by stalkers from cases reported to and investigated by New York City Police Department's Computer Investigation & Technology Unit from 1996 to 2000. Intimate partner stalking is not specifically addressed, however barriers to law enforcement holding cyberstalkers accountable including jurisdictional laws, internet service provider policies, and anonymizing tools are covered. <http://www.fbi.gov/publications/leb/2003/mar03leb.pdf>

Technology Safety Planning with Survivors: Tips to Discuss if Someone You Know is in Danger /Un Plan de Protecci n de la Tecnolog a para las(os) SobrevivientesAuthor: Safety Net, NNEDV (2003, 2004 revised, in English and Spanish) **Description:** This tip sheet provides technology related safety planning strategies for survivors, including telephones, GPS, computers, and the Internet.

Tips for Survivors of High-Tech Abuse and Stalking /Consejos para las(os) Sobrevivientes del Abuso y del Acoso de la Alta-Tecnolog aAuthor: Safety Net, NNEDV (2003, in English and Spanish) **Description:** This handout is designed for survivors and focuses on planning for safety, as well as collecting evidence in complex stalking via technology situations. The document reinforces the key role that a victim plays in identifying methods of technology stalking, provides a sample stalking log, and other documentation examples for a victim of stalking via technology.

Web Wise Women: Part 1 - Minimizing information published about you on the World Wide Web /Mujeres Sabias en la Web. Parte 1 - Disminuyendo la informaci n que ha sido publicada en el World Wide WebAuthor: Safety Net, NNEDV (2003, in English and Spanish) **Description:** This document is designed for survivors of intimate partner stalking who are trying to prevent their private information from being published to the Internet. Information regarding online search engines, court and government websites, private websites, and information brokers/sellers is covered.

Website Safety Alerts: Tips for Advocacy OrganizationsAuthor: Safety Net, NNEDV (2002) **Description:** This document summarizes changes victim advocacy organizations can make to their websites to better educate victims/survivors about computer and Internet monitoring.

Appendix C: A Handout For Survivors

- Technology Safety Planning with Survivors

While Appendix A and B are intended to accompany this paper, Appendix C (following) can be distributed separately from the attached paper. Feel free to share the following technology safety plans with victims, advocates, and allies.

Technology Safety Planning with Survivors

Tips to discuss if someone you know is in danger. Technology can be very helpful to victims of domestic violence, sexual violence, and stalking, however it is important to also consider how technology might be misused.

1. **Trust your instincts.** If you suspect the abusive person knows too much, it is possible that your phone, computer, email, or other activities are being monitored. Abusers and stalkers can act in incredibly persistent and creative ways to maintain power and control.
2. **Plan for safety.** Navigating violence, abuse, and stalking is very difficult and dangerous. Advocates at the National Domestic Violence Hotline have been trained on technology issues, and can discuss options and help you in your safety planning. Local hotline advocates can also help you plan for safety. (National DV Hotline: 1-800-799-7233 or TTY 800-787-3224)
3. **Take precautions if you have a "techy" abuser.** If computers and technology are a profession or a hobby for the abuser/stalker, trust your instincts. If you think he/she may be monitoring or tracking you, talk to a hotline advocate or the police.
4. **Use a safer computer.** If anyone abusive has access to your computer, he/she might be monitoring your computer activities. Try to use a safer computer when you look for help, a new place to live, etc. It may be safest to use a computer at a public library, community center, or Internet cafe.
5. **Create a new email account.** If you suspect that anyone abusive can access your email, consider creating an additional email account on a safer computer. Do not create or check this new email from a computer your abuser could access, in case it is monitored. Use an anonymous name, and account: (example: bluecat@email.com, not YourRealName@email.com) Look for free web-based email accounts, and do not provide detailed information about yourself.
6. **Check your cell phone settings.** If you are using a cell phone provided by the abusive person, consider turning it off when not in use. Also many phones let you to "lock" the keys so a phone won't automatically answer or call if it is bumped. When on, check the phone settings; if your phone has an optional location service, you may want to switch the location feature off/on via phone settings or by turning your phone on and off.
7. **Change passwords & pin numbers.** Some abusers use victim's email and other accounts to impersonate and cause harm. If anyone abusive knows or could guess your passwords, change them quickly and frequently. Think about any password protected accounts - online banking, voicemail, etc.

8. **Minimize use of cordless phones or baby monitors.** If you don't want others to overhear your conversations, turn baby monitors off when not in use and use a traditional corded phone for sensitive conversations.
9. **Use a donated or new cell phone.** When making or receiving private calls or arranging escape plans, try not to use a shared or family cell phone because cell phone billing records and phone logs might reveal your plans to an abuser. Contact your local hotline program to learn about donation programs that provide new cell phones and/or prepaid phone cards to victims of abuse and stalking.
10. **Ask about your records and data.** Many court systems and government agencies are publishing records to the Internet. Ask agencies how they protect or publish your records and request that court, government, post office and others seal or restrict access to your files to protect your safety.
11. **Get a private mailbox and don't give out your real address.** When asked by businesses, doctors, and others for your address, have a private mailbox address or a safer address to give them. Try to keep your true residential address out of national databases.
12. **Search for your name on the Internet.** Major search engines such as "Google" or "Yahoo" may have links to your contact information. Search for your name in quotation marks: "Full Name". Check phone directory pages because unlisted numbers might be listed if you have given the number to anyone.

The copyright of this particular part of the article belongs to The NNEDV Fund 2003. Created 6/03, Revised 5/04 by Cindy Southworth, Shawndell Dawson, and Cynthia Fraser with Safety Net: the National Safe & Strategic Technology Project at the National Network to End Domestic Violence www.nnedv.org

References

- Associated Press. (1995, March 30). Man charged in caller ID killing. *Dallas Morning News*, p. A33.
- Bahm, T. (2003, Summer). Eliminating "cyber-confusion". *Newsletter of the Stalking Resource Center*, 3(2) [Electronic Version]. Retrieved August 30, 2004, from the National Center for Victims of Crime website: http://www.ncvc.org/src/main.aspx?dbID=DB_Eliminating_Cyber-Confusion251
- Brewster, M. (2003). Power and control dynamics in prestalking and stalking situations. *Journal of Family Violence*, 18(4), 207-217.
- Cellular Telecommunications & Internet Association. (2004). CTIA's semi-annual wireless industry survey, June 1985 - June 2004 [Electronic Version]. Washington DC: Author. Retrieved February 20, 2005, from <http://files.ctia.org/pdf/CTIAMidyear2004Survey.pdf>

- CyberAngels. (1999). Retrieved February 20, 2005, from <http://www.cyberangels.org>
- Dean, K. (2000). The epidemic of cyberstalking. *Wired News*. Retrieved February 20, 2005, from <http://www.wired.com/news/politics/0,1283,35728,00.html>
- Department of Justice. (1999). 1999 Report on cyberstalking: A new challenge for law enforcement and industry [Electronic Version]. Washington, DC: U.S. Department of Justice, Office of the Attorney General. Retrieved July 7, 2004, from <http://www.usdoj.gov/criminal/cyber-crime/cyberstalking.htm>
- Department of Justice. (2001). Stalking and domestic violence: Report to Congress (NCJ 186157). Washington, DC: U.S. Department of Justice.
- Ellison, L., & Akdeniz, Y. (1998, December). Cyber-stalking: The regulation of harassment on the Internet. [Electronic Version]. *Criminal Law Review, December Special Edition: Crime, Criminal Justice and the Internet*, 29-48. Retrieved February 20, 2005, from http://www.cyber-rights.org/documents/stalking_article.pdf
- Finn, J. (2001). Domestic violence organizations online: Risks, ethical dilemmas, and liability issues. Retrieved July 7, 2004 from http://www.vaw.umn.edu/documents/commissioned/online_liability/online_liability.pdf
- Finn, J. (2004). A survey of online harassment at a university campus. *Journal of Interpersonal Violence*, 19(4), 468-483.
- Fisher, B. S., Cullen, F. T., & Turner, M. G. (2000). The sexual victimization of college age women (NCJ 182369). Washington, DC: U.S. Department of Justice, National Institute of Justice and Centers for Disease Control and Prevention.
- Greenfeld, L. A., Rand, M. R., Craven, D., Klaus, P. A., Perkins, C. A., Ringel, C., et al. (1998). Violence by intimates: Analysis of data on crimes by current or former spouses, boyfriends, and girlfriends (NCJ 167237). Washington DC: U.S. Department of Justice.
- H.E.S. v. J.C.S., 175 N.J. 309, 815 A.2d 405 (Sup. Ct. February 6, 2003). Retrieved February 20, 2005, from <http://lawlibrary.rutgers.edu/decisions/supreme/a-132-01.opn.html>
- Jenson, B. (1996). Cyberstalking: Crime, enforcement, and personal responsibility in the on-line world. Retrieved May 30, 2004, from <http://www.sgrm.com/art-8.htm>
- Kranz, A. L. (2001). Survivors of intimate violence seek help online: Implications of responding to increasing requests. Retrieved July 7, 2004, from <http://www.vaw.umn.edu/documents/10vawpaper/10vawpaper.html>
- Lamberg, L. (2001). Stalking disrupts lives, leaves emotional scars. *Journal of American Medical Association*, 286(5), 519-523. Retrieved June 18, 2004, from <http://jama.ama-assn.org/cgi/content/full/286/5/519>

- Laughren, J. (2000). Cyberstalking awareness and education. Retrieved May 30, 2004, from <http://www.acs.ucalgary.ca/~darbent/380/webproj/jessica.html>
- Lee, R. (1998). Romantic and electronic stalking in a college context. *William and Mary Journal of Women and the Law*, 4, 373-466.
- McFarlane, J. M., Campbell, J. C., Wilts, S., Sachs, C. J., Ulrich, Y., & Xu, X. (1999). Stalking and intimate partner femicide. *Homicide Studies*, 3(4), 300-316.
- Madden, M., & Rainie, L. (2003). America's online pursuits: The changing picture of who's online and what they do. Retrieved July 1, 2004, from http://www.pewinternet.org/pdfs/PIP_Online_Pursuits_Final.PDF
- Maxwell, A. (2001). Cyberstalking. Retrieved May 30, 2004, from http://www.netsafe.org.nz/Doc_Library/cyberstalking.pdf
- National Center for Victims of Crime. (2004). Stalking [Electronic Version]. Problem-Oriented Guides for Police: Problem-Specific Guides Series No. 22. Washington DC: U.S. Department of Justice, Office of Community Oriented Policing Services. Retrieved February 20, 2005, from <http://www.cops.usdoj.gov/mime/open.pdf?item=1042>
- National Criminal Justice Association. (1993). Project to develop a model anti-stalking code for states. Washington, DC: U.S. Department of Justice, National Institute of Justice.
- Ogilvie, E. (2000, September). Cyberstalking. *Trends & Issues in Crime and Criminal Justice*, 166 [Electronic Version]. Retrieve May 30, 2004, from <http://www.aic.gov.au/publications/tandi/ti166.pdf>
- Orland, K. (2003, February 6). Stalker victims should check for GPS. *CBS News.com*. Retrieved July 7, 2004, from <http://www.cbsnews.com/stories/2003/02/06/tech/main539596.shtml>
- Safety Net: The National Safe & Strategic Technology Project. (2004). Safety net training curriculum: Technology, advocacy, and victim safety. Washington, DC: The National Network to End Domestic Violence Fund.
- Spitzberg, B., & Hoobler, G. (2002). Cyberstalking and the technologies of interpersonal terrorism. *New Media & Society*, 4(1), 71-92.
- Stalking Resource Center. (2003, Summer). Stalking technology outpaces state laws. *Stalking Resource Center Newsletter*, 3(2), 1, 3-4 [Electronic Version]. Retrieved July 7, 2004, from <http://www.ncvc.org/src/main.aspx?dbName=DocumentViewer&DocumentID33500>
- Tjaden, P., & Thoenes, N. (1998). Stalking in America: Findings from the National Violence Against Women Survey (NCJ 169592). Washington, DC: U.S. Department of Justice.

- Webster, K. (2003, December 1). Victim advocates want names, addresses, records offline. USA Today. Retrieved February 20, 2005, from http://www.usatoday.com/tech/news/internetprivacy/2003-12-01-victim-privacy_x.htm
- Wendland, M. (2001, September 6). State targets cyber spies: Belleville man accused of electronic voyeurism. Detroit Free Press. Retrieved July 8, 2004, from http://www.freep.com/money/tech/spy6_20010906.htm
- Working to Halt Online Abuse (WHOA). (2003). Online harassment statistics: Prior contact - 2000-2004. Retrieved on June 28, 2004, from <http://www.haltabuse.org/resources/stats/relation.shtml>