TECHNOLOGY, STALKING AND DOMESTIC VIOLENCE VICTIMS

Cindy Southworth and Sarah Tucker*

The Digital Age is bringing many opportunities to survivors of abuse and their advocates.¹ Across America, victims of domestic violence are using the revolutionary tool of the Internet to map roads to new lives by reaching out to shelters, researching restraining orders, and finding housing and employment opportunities. However, at the same time, advancements in technology are posing unique challenges to enhancing victim safety. Abusers regularly use a variety of technologies to stalk current and former intimate partners, ranging from phones to mapping to computer technologies. Some abusers install global positioning systems to stalk their victim’s real-time locations with extraordinary accuracy, while others use telephones to leave hundreds of messages in a single day. Other stalkers use technologies like caller ID during a relationship to monitor their partner’s calls, and to locate her after she has fled. Still others use online databases, electronic records, and web search engines to locate, track, and harass former partners. Regardless of the tool or technology used,

* Safety Net: the Safe and Strategic Technology Project at the National Network to End Domestic Violence Fund.
¹ Since people surviving abuse identify themselves differently, in this article 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. LAWRENCE A. FREENFELD, ET AL., U.S. DEPT OF JUSTICE, NCJ-167237, VIOLENCE BY INTIMATES: ANALYSIS OF DATA ON CRIMES BY CURRENT OR FORMER SPOUSES, BOYFRIENDS, AND GIRLFRIENDS, at iii (1998), available at http://www.ojp.usdoj.gov/bjs/pub/pdf/vi/pdf (last visited January 29, 2007).
perpetrators have the same primary goal: abusing power to gain and maintain control over their victims.

I. 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. Computer Monitoring Software and Hardware

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.\(^2\)

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. One man admitted that he “e-mailed his ex-wife Spyware that automatically downloaded to her computer, which allowed him to secretly monitor her online communications and read her e-mail.”\(^3\)

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

---

1 Mike Wendland, State Targets Cyber Spies: Belleville Man Accused of Electronic Voyeurism, DETROIT FREE PRESS, Sept. 6, 2001 at 1B.

in use. Additionally, if the victim installs new programs or clears all computer trails, this could cause suspicion and increase danger.

Spyware is not just for desktop and laptop computers anymore. As more and more people are using cell phones or handheld devices to access the Internet, spy software has kept up with this trend. In March of 2006, Vervata began advertising FlexiSpy which “captures call logs, text messages and mobile Internet activity, among other things.” It sells for $49.95 and is advertised “as a tool to monitor kids and unfaithful spouses.”

In addition to software programs, stalkers use hardware devices called “Keystroke Loggers” that are inserted into a USB port or 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. However, abusers must have physical access to a victim’s computer in order to use these devices, as they must physically retrieve the information stored on them.

B. The Internet

“A police officer seeking revenge against a former girlfriend hacked into the woman’s 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.” Another abuser changed his wife’s email password and sent threatening messages to himself from her email account. Then he took the printed messages to the police and asked them to arrest her. Another abuser discovered that his victim was planning to flee by viewing an email she thought she had

---


5 Id.

6 Erik German, Officer Charged with Cyber-Stalking His Ex, L.A. TIMES, Apr. 4, 2006, at A19.
deleted. However, she did not realize that she had to empty her “deleted items” folder. He discovered her escape plan by checking this folder, and he killed her.7

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.8

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. A Montgomery County, Pennsylvania Court went a step further, publishing the names and addresses of victims (and their children) who obtain protection orders to the web.9

The mere existence of a victim’s name on a website could lead a batterer or stalker to a victim’s new community, if not

---

8 Id.
her exact address. If a victim moves to a new town to start a new life away from a batterer, she might be found if an online court index lists only her name on the Internet. Failing to expressly exclude victim and witness identities from web or remote access will mark these victims and witnesses for continued violence and harassment by the batterer. This encroachment on privacy and the resulting threat to personal safety will discourage victims of domestic violence from seeking protection from their abusers, just as it will discourage witnesses from helping to end the violence through their testimony.

Most public filings can give abusers the information they need to track their victims. Posting such filings on the Web increases their utility and accessibility for some, but also increases the chance that victims will be found. For example, if a victim of domestic violence flees her abuser in Virginia, relocates to Texas, buys property, and files her land record with a court that posts such records on the Web, her abuser can find her with a simple, national HTML search. Many of life’s most important events involve the court system. In a jurisdiction where the court posts records on the Internet, a victim of domestic violence must weigh the benefits of the activity against the possibility that her attacker will locate her.

C. Location & Surveillance Technologies

I’ve been tracking my girlfriend through her mobile phone. I can see exactly where she is, at any time of day or night, within 150 yards, as long as her phone is on...... On the website, I see the familiar number in my list of “GSM devices” and I click “locate”. A map appears of the area in which we live, with a person-shaped blob in the middle, roughly 100 yards from our home..... There is no trace of what I’m doing on her phone..... I can’t find anything in her mobile that could possibly let her know that I’m checking her location. As devious systems go, it’s foolproof. I set up the website to track her at regular intervals, take a snapshot of her whereabouts automatically, every half hour, and plot her path
on the map, so that I can view it at my leisure.\textsuperscript{10}

Although Goldacre had his girlfriend's permission to track her for an article he wrote, his account illustrates how incredibly easy it is to track someone via their cell phone signal or a GPS chip. 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, abusers can track their victims with Global Positioning Systems (GPS) that use satellite receivers to provide precise real-time worldwide positioning. These devices vary by price, size, and appearance, ranging from a small black box to a hand-held unit to a small chip in a wristband. 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 . . . .\textsuperscript{11} Since 2002, GPS systems have become less expensive and many are being marketed as ways for parents to track their teen drivers. The lower cost and increased availability has made them available to more of the general public, stalkers included. This may be one reason for the sharp increase in the number of GPS stalking cases reported by the media in recent years.

While many cell phones now have GPS chips in them to aid 911 operators in identifying their location, older phones do not. Yet, these can still be located. A variety of services operate on the Internet, offering to locate a phone though the cell towers it is accessing or through an internal GPS chip, often using illegal means to provide this information to anyone willing to pay.


D. Cameras

Stalkers use small hidden cameras to monitor their victims and learn their routines. 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.12

As web cameras become increasingly popular, these too are being used by perpetrators. With the recent increases in the use of high-speed Internet service, many people are using an "always on" Internet connection.13 As if they weren't scary enough, many spyware programs also allow a user to remotely activate a webcam, allowing an abuser to turn on the camera at anytime, using it as a window into the living room of the victim.

II. PHONE TECHNOLOGY

While technology has greatly enhanced our ability to communicate by providing us with a wide variety of newer and better tools, telephones remain the one of most prevalent and least expensive communication technologies. Because of this, many abusers rely on telephones as their first weapon to harass their victims, through repeated and harassing phone calls or threatening messages left in voicemail and on answering machines.

While harassing calls made using a traditional land line telephone (vs. a cellular phone) can be traced via phone company records, there's no guarantee that the phone at the other end will have any connection to the perpetrator. It could be at a friend's home, hotel, or even a pay phone at the local gas

station. Until recently, tracing cell or wireless phone calls has been somewhat easier as these phones generally belong to an individual and have a credit card number and address associated with them. However, the advent of pre-paid phones has made this increasingly difficult. If a phone card or prepaid cell phone 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 more difficult to trace.

A. Caller ID

Most cell phones and many Caller ID enabled phones keep an internal record of incoming and outgoing calls, which abusers often use to monitor survivors’ phone use. In Rhode Island, one abuser assaulted his wife after finding the shelter phone number in her cell phone call history; as a result she did not attempt to leave her husband for another year.14 Caller ID also allows abusers to stalk and locate their victim after the relationship has ended. Soon after Caller ID was first available, an abuser in Texas used Caller ID to track down his former girlfriend and murdered her.15

B. Fax Machines

Abusers and stalkers have used the fax header on faxed documents to locate their victims. 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 phone number and location of his victim and she had to relocate again.16

14 SOUTHWORTH, supra note 7, at 6.
16 SOUTHWORTH, supra note 7, at 6.
C. TTY/TTD

Teletypewriters (TTY) and Telecommunications Devices for the Deaf (TTD) are text based phones 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 their 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 emerged 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.17

III. CONCLUSION

As devices continue to meld, the distinctions currently made between computers, phones, fax machines, cameras, and TTYs are quickly disappearing. Many handheld devices allow the user to search the Internet, send instant messages, take photos, and send text messages. Some people use web cameras and online chat websites (like AOL’s AIM) to simultaneously text message and view others. Emerging technologies like VoIP, a popular method of cheap long distance phone via the Internet, further blur a user’s sense between phone and online communication. The recent increase in the popularity of chat rooms, forums, and blogs has been evident too, as more survivors use these as vehicles to share their stories and seek support. All of these technologies are also increasingly used by abusers to harass, deceive, monitor, and stalk survivors.

As stalkers continue to increase their use of technology, it is vital that communities are equipped to respond to these crimes. In an age where stalkers use search engines to track them down, victims need to be able to relocate safely. As more records are published on the Internet, advocates must educate

17 Id.
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 ally building are critical to lessening the barriers that victims of technology stalking encounter.

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. Intimate partner stalkers are persistent and resourceful, but so are the advocates and survivors fighting against them.