TECHNOLOGY ISSUES FOR VICTIMS AND VICTIM SERVICE PROVIDERS

PRESENTED BY:
ALLISON VACHON
OBJECTIVES

*Upon completion of this module the participant will be able to:*

- Better understand the overall technology issues that may affect victim safety.
- Better understand the technology issues that should be taken into account in safety planning with victims.
- Better understand the technology issues that should be covered by the practices, protocols and procedures of victim services agencies and advocates in their work with victims.
Technology Issues for Victims and Victim Service Providers

Maine/NH Victim Assistance Academy
May 2012

Allison Vachon, Investigator
NH Attorney General’s Office

Allison Vachon
Internet Crimes Unit
Internet Crimes Against Children (ICAC) Task Force

“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
Technology and Advocates

- Advocates and victims use technology on a daily basis
- Along with the benefits, the use of technology has many risks that may impact victim safety and advocate confidentiality

Topics for Discussion

- An overview of the relevant technology issues
- Technology issues to consider in safety planning with victims
- Technology issues to consider for agency practices and protocols
- A better overall understanding of these technology issues

Statistics

- 3.4 million people are stalked annually (in the US)
- 1 in 12 women has been stalked in their lifetime
- 1 in 45 men has been stalked in their lifetime
- Over three quarters (78%) of stalking victims are female and most (87%) stalking perpetrators are male
- Electronic stalking often leads to, or is accompanied by, physical stalking, and explicitly or implicitly threatens physical stalking (Lee, 1998)
Different forms of Stalking through the Use of Technology

- Telephones
- Cellular Phones
- Fax machines
- Spoofing
- E-mail
- Instant Messaging (IM)
- Global Positioning Systems (GPS)
- Hidden Cameras
- Computer Monitoring Devices
- Online Databases

Telephones – Cordless Phones

- Cordless phones are susceptible to having calls intercepted by scanners and to “crosstalk” on devices such as baby monitors and other cordless phones up to a mile away (1/4 mile is a “normal” range)

- If you switch during your call to a corded phone and hang up the cordless phone, the cordless phone’s base continues to transmit the call unless you unplug the base/transmitter
Cordless Phones – Recommendations

- Do not use cordless phones unless really necessary
- Advocates should inform victims of the possible risks of using cordless phones
- If it is necessary to use a cordless phone, avoid mentioning any details and identifying information that would compromise victim safety or confidentiality

Telephones – Corded Phones

- Corded phones may be tapped from inside or outside the building. The tap may be hooked directly to a tape recorder or it may transmit the call to a remote recording device/receiver.
- Caller ID boxes may be installed without the victim’s knowledge (i.e. in the basement)
- Recommendation: Use caution where there is a known safety risk. Avoid mentioning identifying information and planning details.

Telephones – VOIP

- Voice Over Internet Protocol is broadband Internet based phone service (i.e. Vonage)
- VOIP phones do not always connect to 911. Victims using VOIP should register their primary address with E-911.
- You can’t tell where someone is calling from
- Easily tapped as it is unencrypted
Telephones – VOIP

- VOIP software can be configured to unblock the “Calling Party Number” with each call
- Call logs, voicemail, etc. are on the computer
- Doesn’t work well with many alarm systems

Telephones – TTY/TTD

- Phones for the hearing impaired/deaf
- Devices often record and save exact history of conversations, making it easier for stalkers to monitor victim’s conversation
- Abuser can impersonate victims by using their TTY to seek information about their activities

TTY/TID – continued

- Example – 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 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 the charges. (Safety Net, 2004)
Telephones – General

- All agency phone and fax lines and any other phone lines used by advocates should have their lines blocked for Caller ID and be TESTED REGULARLY to ensure it is in place.
- Safety planning and agency policies should include education and planning in regards to Caller ID and phone use in general (if or when to call, *69, redial, etc.)
- Verify the identity of the caller before discussing anything of substance.

Safety planning and agency policies should include education and planning in regards to Caller ID and phone use in general (if or when to call, *69, redial, etc.)

- Verify the identity of the caller before discussing anything of substance.

Telephones – General

- Advise clients that most phone companies provide the capability for online billing records for phones, calling cards, pre-paid cell phones, etc. The abuser may have access to these records or pay a service to get them.
- Stalkers may access voicemail and answering machine messages remotely.
- Stalkers may use reverse lookup to find who a phone number belongs to (i.e. AnyWho.com)

Cellular Phones

- Abusers monitor their victim’s cell phone use through the call history and through billing records. Most cell phones keep an internal record of incoming/outgoing calls.
- Use phone-based instant messaging and text messaging to maintain constant access to their partners or ex partners.
- Can use new location based services to track the location of their victims.
- Newer digital cell phones (2.4 GHz and up) are much more secure but they can switch to the easily intercepted analog mode depending on antennae coverage (especially in rural areas).
Some cell phones can be programmed to answer calls automatically. If the ring is also silenced, the abuser can “plant” the phone, call it, and hear everything going on in the room. The cell phone becomes a “bug” the abuser can call at will.

“Spy Phone” cells can monitor both sides of all calls and even all conversations when the phone is hung up. Still very expensive.

Example – 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)

Enhanced 911 requires cell phones to have GPS capability. This is great if emergency dispatch needs to pinpoint your distress call.

However, this capability can be used by perpetrators to track and locate victims. Subscription services are available that will allow someone to go online and pinpoint the exact real-time location of a cell phone, sometimes even when it is turned off. Some of these services will also provide a travel “history” of all movements.
Cell Phone - Recommendations

- Use newer, digital cell phones (2.4 GHz+) and if possible set so GPS works only with 911 calls
- Especially avoid using cell phones anywhere you are known to frequent (i.e. home, office)
- Use caution where there is a known safety risk. Avoid mentioning identifying and planning details.
- When fleeing/leaving, leave the cell phone behind. Cell phone donation programs – no plan required to dial 911.

Spy Phones - Software

- Call Magic Features: (Ground breaking technology)
- Silently Answer Incoming Call from a pre-defined number
- Runs in “Real Background” mode
- Automatically starts when is switched on

World Tracker

- The next frontier in warrant-free surveillance is upon us, and it's open to everyone. A UK service called World Tracker uses cell tower data (or GPS, when available) to track the location of just about any cell phone.
- Just enter the number you want to track into the service's handy Google Maps-based interface, and you'll be able to zoom in on the device's location, with accuracy somewhere between 50 and 500 meters.
World Tracker

World Tracker turns anyone into a cellphone spy

- Spoofing via spoof cards or websites allows victims or perpetrators to hide their location and identity – even disguise their voice
- They can display a different number than the one they are calling from and some offer a call recording option
- Websites such as Camophone.com utilize VOIP and keep no records of callers or calls
- Also see Spoofcard.com, Telespoof.com, itellas.com

**SpoofCard calling cards offers you the ability to change what someone sees on their caller ID display when they receive a phone call.**

**Key Benefits:**
- Make calls truly private
- Ability to record calls
- Change your voice
- Fun and inexpensive
- Easy to use and fast to set up

**Instant Access!**

**SPOOFCARD FEATURES:**
- Caller ID Spoofing
- Voice Changer
- Call Recording
- Web Control Panel

No computer needed! Simply dial the toll free number from the calling card you purchased.

1. Enter your pin number.
2. Enter Destination number.
3. Enter Any Caller ID Number you wish to display.
4. Choose the voice you would like to use.
5. Your call is connected using the specified Caller ID Number.

As an added bonus, we offer you the option to record your conversation for **FREE** which you can later retrieve by logging in to your control panel or calling our 800 number from anywhere.

In addition, we also offer the ability to change your voice to sound like a man, a woman or yourself for **FREE**.
Fax Machines

- Be aware that fax machines can contain identifying information in the “fax header”
- If sending paperwork to/from attorneys, this can give victim location information to the abuser
- Verify identity of sender
- Do not retain faxes that may compromise confidentiality and security

Location and Surveillance Technologies

Newest Trends

- Used to be abuser would check car odometers to measure mileage and monitor victim’s daily activities
- Now tools ranging from inexpensive digital cameras to high-tech streaming video cameras and global positioning systems (GPS) are being used by such perpetrators
Global Positioning Systems (GPS)

- Abusers use GPS that use satellite receivers to provide precise real-time worldwide positioning to locate and follow victims.
- Because they work off satellites, they perform even in the most remote areas.
- The devices can vary in price, size, and appearance.
- New services that map the location of "friends" are growing in popularity (i.e. MapQuest Find Me or Follow Us).

GPS - continued

- GPS technology can also be part of anti-theft services for vehicles such as OnStar.
- Stalker could secretly install GPS device under hood of victim's vehicle and stalk for months.
- Advocates should educate victims on checking for devices in their vehicles.

GPS Locator Sample
Our SlimTRAK GPS ULTRA Tracker makes all others obsolete!

Google & Windows Live Satellite Mapping with Birds Eye View is available!

Weighing in at only 7.2 ounces, the all new SlimTRAK real time tracking system makes all others obsolete! No more complicated wiring or GPS antenna mounting. Due to new state-of-the-art "high sensitivity antenna" technology, the very small SlimTRAK tracker is completely self contained, including 4 standard "AA" batteries that power the unit for a full 3 months. Of course, if you prefer a permanent installation, connection assembly with battery back up is also available.

INSTALLS IN SECONDS: Once activated, SlimTRAK can be installed just about anywhere in the vehicle, under seat, in glove box, or any other convenient location. (Not recommended for use in a trunk.) For covert applications, our custom fitted waterproof magnetic case allows for quick installation under the vehicle or under hood. Unit can easily be moved from one vehicle to another. Also great for protecting heavy equipment, boats, industrial equipment and dozens of other items.

EXTREMELY EASY TO USE: No rocket scientist need handy! Unit operates using GPS and GSM communication technology. To track your vehicle, simply access the SlimTRAK website from any internet active computer, type in your password, and a detailed map with tracking information appears. Info includes time, speed of vehicle, street address of vehicle and last stop. Updates as little as every 2 minutes, to keep you on target. Unit can be programmed for faster or slower update frequency, if desired. Toll free customer support assures that all your questions be answered promptly.

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Address</th>
<th>Plate#</th>
<th>License Plate</th>
<th>Miles</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>08/05/06</td>
<td>111 River Rd., ME 04629</td>
<td>A123XYZ</td>
<td>1234567</td>
<td>123</td>
<td>-</td>
</tr>
<tr>
<td>09/05/06</td>
<td>222 Main St., NY 12345</td>
<td>CD789UV</td>
<td>987654321</td>
<td>789</td>
<td>-</td>
</tr>
<tr>
<td>10/05/06</td>
<td>333 Elm Ave., CA 90210</td>
<td>EFGHIKLM</td>
<td>123456789</td>
<td>987</td>
<td>-</td>
</tr>
</tbody>
</table>

Satellite View: When you click on one of the dots, location data is displayed.
GPS - Recommendations

- If a victim notices their abuser showing up in places that they can't understand how the abuser knew they were there, GPS tracking may be occurring. Try to locate a GPS device and/or get a new cell phone.

- If a GPS device is suspected or located as “planted” on the victim, law enforcement may be able to use that to trap the abuser

Location-based Social Networking

What is it?
- Social networking that uses geographic services and technologies allowing users to communicate and find people with similar interests

How does it work?
- On mobile devices, applications utilize the mobile network and GPS to identify the location of the mobile device
- Mobile social networks often rely on texted information or enabling of phone tracking

Location-based Social Networking

- Terminology
  - Location-tagging or geo-tagging
  - Check-ins
  - Location-Aware

- Problem is having these applications connected to Facebook and Twitter
Hidden Cameras

- Stalkers use small hidden cameras to monitor their victims and learn their routines
- Use information they gather to exert power and control over them
- Small wireless high resolution cameras can be hidden in smoke detectors, lamps, or behind a pin-sized hole in a wall and can be activated remotely

Hidden Cameras - continued

- Example – 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)

Spy Cam Sample

Air Purifier Camera - 2.4 GHz Wireless Spy Cam

Model: SCI-AIRPUR24

Suggested B&W: $469.99
B&W Price: $349.99

Suggested Color Price: $449.99
Spy Cam Sample

Computer and Internet Technology

- Any Internet use leaves numerous traces on the computer that can easily reveal what sites were visited. Even if you clear the browser history file & locator bar and delete all the “cookies”, there are still traces of the Internet sites buried in various places (i.e. cache files). These trace “footprints” of Internet use are fairly easy to find and virtually impossible to completely eliminate.

- WiFi and Bluetooth connections can be accessed within their range to steal data, tap into communications or “hijacked” and run by the abuser

Computer and Internet Technology - Continued

- Computer monitoring software
- “Spyware” originally developed to monitor children’s Internet use
- Allows abuser to monitor computer and Internet activities and discover a victim’s efforts to escape or access help
- Can be installed remotely or by physically accessing the victim’s computer
- Programs can send regular emails to the stalker reporting all of the victim’s computer activity, including all emails sent and received and all web sites visited
- Spyware is transparent to the user
- Spyware protection and/or detection software does not always work
Spyware Sample

Computer and Internet Technology - Continued

- Keystroke Logging Hardware

- Hardware devices that are inserted between the keyboard cable and the back of the computer

- Contain small hard drives that record every key typed, including all passwords, PINs, websites, and email

- Spyware detection programs cannot detect

Keystroke Logging Hardware
Computer and Internet Technology - Recommendations

- If at all possible victims should be advised not use a computer that their abuser has access to for any Internet use related to their victimization. Use a friend’s or one from a library, school, etc.

- Victim service agencies should post highly visible warnings on every page of their websites and include directions, or links to directions, on how to remove the most obvious “footprints”

E-mail & Instant Messaging (IM)

- Abusers use to threaten victims and impersonate them
- Can send malicious spyware or viruses as email attachments
- Examples –
  - One abuser changed his wife’s email password and sent threatening messages to himself from her email account then took the printed messages to police and asked them to arrest her.
  - Another killed his wife after discovering she was planning to flee. He learned of her escape plan in an email in her “deleted email folder”. (Safety Net, 2004)

E-mail & IM - continued

- E-mail and Instant Messaging are not confidential methods of correspondence. They are subject to interception, impersonation and hacking.
- Victims should shut off their Bluetooth functionality unless they are using it and/or set the device (i.e. headset) to “hidden” to make it much more difficult to hack into
- Victims should not use a computer their abuser has access to for e-mail or IM’ing
- Victims should use free, web based e-mail accounts set up with false names, etc.
E-mail & IM - Recommendations

- Victims should not have e-mail user names and passwords with ties to themselves. Change passwords often.
- All should verify the identity of senders. Do not open attachments from unknown sources.
- Do not retain email electronically or on paper that would threaten safety or confidentiality.
- Ensure that victims are aware that abusers may impersonate them via emails or IM's to friends, relatives, employers, etc.

E-mail & IM Recommendations - continued

- Never use victim/client names and other identifying information in e-mail.
- E-mail and IM policies should be included in your agency policies.
- Agencies should not have victim specific information on computers that are directly or indirectly (i.e. via LAN) connected to the Internet.

Computer Databases

- A name and SSN is all that is needed to get a victim's credit report showing the most recent employment, address, bank accounts, etc.
- Governmental agencies continue to make more "public information" available online (i.e. court records, motor vehicles, tax data, voter registrations, etc.)
- Retail chain stores increasingly database customer information (dept. stores, grocery, video rental, oil change, etc.)
Computer Databases - continued

- To the extent that some of this information is not available to the general public, for a fee, there’s an Internet based detective agency or service that will get it for the abuser (i.e. the Amy Boyer case, defendant Liam Youens)

- Sometimes simple, easy to use, and inexpensive “hacker” software can be used to access non-public database information

Computer Databases - Recommendations

- Victims not wanting to be “found” should enroll in their State’s Address Confidentiality Program (if available)

- Do not give out phone numbers or have them printed on personal checks

- Google the victim’s name to see what online information is currently available

Computer Databases Recommendations - continued

- Also check www.zabasearch.com or www.pipl.com or www.123people.com

- Free real time people search tool that looks into nearly every corner of the web, claims to "thoroughly invade someone’s privacy"

- Victim specific information should not be stored on a computer that is hooked to the Internet
• Victims should not use stores that database your name and address or use customer discount cards. These names and addresses can be hacked or sold.

• Victims in hiding might consider feeding disinformation to public databases to promote the appearance that they are living elsewhere.

Advocacy Response – General Recommendations

• Vital that advocates continue to support the strategies survivors have been using to help them navigate the abuse and stalking in their lives.

• Important to work with victims to plan for safety around technology and stalking.

• Technology changes rapidly and abusers are adept at misusing new tools.

• Importance of discussing with victims that law enforcement involvement can often escalate the abusers violent behavior.

Strategies for Advocates

• Educate survivors about new tools and the potential use of technology to stalk without prohibiting access to technology.

• Share information about technology safety risks in ways that are relevant to the concerns raised by the survivor.

• Some may feel relieved to finally figure out why their stalkers are able to know everything they do.
Strategies for Advocates - continued

- Technology stalking and safety can be considered as a topic for discussion in DV or stalking support groups.

- If a victim wants to report crimes to police, LE may have a short window to collect digital evidence since many companies only retain info for a limited amount of time.

- Given that abusers work in every field, evaluate data collection and sharing policies to keep victim data out of the hands of stalkers, abusers, and members of the public.

Safety Planning Tips

- Phones
  - Screen calls with caller ID and answering machines
  - Document harassing calls, call trace
  - When calling victims use caller ID block
  - Call ahead before sending faxes, delete fax header
  - Use password or phrase when using TTY to confirm ID
  - Determine if "location services" has been added to cell

Safety Planning Tips - continued

- Location and Surveillance
  - Encourage victims to trust their instinct if they think they're being followed
  - Help them find LE or mechanic to search vehicle for GPS device
  - Talk to survivors about checking their homes for small holes, wiring, or hidden cameras.
Safety Planning Tips - continued

- Computers
  - Encourage victims to use a safer computer, one the stalker does not have access to or know about
  - Encourage not to open attachments from unknown sources

Closing Tips

- DV victims often have trouble believing something other than their partner really loves them but has anger management issues
- Advocates sometimes find it useful to have victims look at the abusing partner’s behavior from the stalking perspective. This can help a victim realize that some of their abuser’s behaviors are cold, calculating and manipulative, not done in the heat of anger

Real Life Stalking Cases

- PORTSMOUTH — A Somersworth man is being held on $2,500 cash bail on a stalking charge alleging he used a global positioning system on his victim’s phone to track her movements and locate her only a day after he was arrested for allegedly assaulting the woman.
  - Police say Michael Barnes, 42, of 56A Market St., breached his bail conditions on previous simple assault charges when he enabled a GPS application on a woman’s phone in an attempt to determine her location.
  - Court paperwork indicates Barnes used the GPS function to determine the victim was staying at an area women’s shelter.
Update on Case Status

- Barnes pled guilty to breach of bail and attempted stalking
- Originally tried to plead guilty to just the breach of bail and place the attempted stalking on file for a year w/o a finding...the judge rejected the plea
- Important to note the victim became aware she was being tracked when her phone carrier sent her a text message notifying her that the GPS function on her cell phone had been activated
- Police say the message listed the phone number that activated the GPS and investigation showed the number it came back to was Barnes' phone
- 12 month jail sentence with all but 32 days suspended on breach of bail, identical and concurrent sentence on the attempted stalking guilty plea

Real Life Stalking Cases

- Michael Barrett plead guilty in ESPN reporter Erin Andrews stalking case
Resources

- National Network to End Domestic Violence
  www.nnedv.org
- The National Domestic Violence Hotline
  Phone 1 (800) 799-SAFE or TTY 1 (800) 787-3224
- Stalking Resource Center (National Center for Victims of Crime)
  www.ncvc.org/src

Thank you all very much for the work that you do...

Allison Vachon, NH Attorney General’s Office
Criminal Justice Bureau (603) 271-3671
allison.vachon@doj.nh.gov

Internet Crimes Against Children Task Force
Portsmouth Police Department
(603) 427-1500
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.