Assisting Survivors with Personal Privacy Management

Digital Technology and Safety Information Booklet – 2012

A joint publication of:

The Pennsylvania Coalition Against Domestic Violence and
The Pennsylvania Coalition Against Rape

PCADV
Pennsylvania Coalition Against Domestic Violence
Prevention • Intervention • Change

PCAR
PENNSYLVANIA COALITION AGAINST RAPE

Introduction

In October 2011, you received a document titled "Tech Top 10 Tips: Social Media Use by Survivors," http://pubs.pcadv.net/clr/112908_Top10Advocacy_socialmedia.pdf, which provided you with some basic advocacy tips for assisting survivors in the age of digital media. This booklet expands on the original technology safety tips, providing additional guidance and best practice information for assisting survivors to protect their safety and preserve their privacy when using social media and personal electronic devices.

> **This booklet is intended to inform advocates in their work, and should not be given directly to survivors.**

Another resource, *Computer and Cell Phone Safety Tips for Domestic & Sexual Abuse Survivors*, accompanies this booklet and is intended for you to give directly to survivors.

Please keep in mind that these tips may not be relevant to all survivors. *In fact, sharing too much of this information may cause additional unnecessary stress to a survivor*. Factors such as the survivor's relationship to the perpetrator and whether there is the possibility of a court case play a huge role in the relevancy of this information. While it is important that all social media/technology users are aware of the information that follows, the way it is shared with a survivor can be based upon the level of privacy concerns for the individual survivor. The answer to the following questions will help you decide how much of the information contained in this booklet you need to discuss with the survivor. For instance, if the survivor is involved in a court case then she or he needs to be aware of how the information contained on social media may come to light as part of that court case. If the survivor is in crisis, then discussing this booklet may not be important at the moment, unless the victimization involves Internet or social media stalking or harassment. Some questions to consider as an advocate:

- Is this a recent assault or recent situation?
- Does the survivor want to pursue criminal charges?
- Does the survivor use social media/technology, and if so how?
- What is the relationship to the perpetrator?
- Have there been any instances of stalking or sexual harassment?
- Is the survivor connected to the perpetrator in any way on social media?

For more information, or for additional assistance, please contact the PCADV Legal Department at 717-671-4767 or PCAR at 717-728-9740.

Overview

It may be particularly dangerous for some survivors to continue to use social media, especially when involved in pending or ongoing legal proceedings. An advocate may advise the survivor that her or his safest strategy is to completely avoid social media because of the threat of exposure, the legal implications, and the opportunity for continued abuse, stalking, and harassment. It may not be realistic for every survivor to stop using technology and social media altogether.

Social media – particularly for younger survivors – may be an essential part of the way she or he communicates. It serves as an important communication tool for many survivors, allowing them to contact and connect with their friends and family that are perhaps not otherwise accessible.

Advocates should warn clients of the types of harm that could result from using social media and other forms of technology. If a survivor has a legal matter pending, such as custody, divorce, or is involved in a criminal proceeding, she or he should also be encouraged to consult with an attorney about social media use.

However, advocates should give survivors strategies for protecting themselves if they choose to keep using social media.

In some cases, such as when a survivor is involved in civil or criminal litigation, it may be safest for the survivor to avoid social media entirely. Comments, pictures, or activities that are posted on the Internet will be there forever and defense attorneys or opposing counsel will be looking for those items to use against the survivor in the litigation.

As appropriate, advocates can provide survivors with the strategies outlined in this bulletin for protecting information if the survivor continues to use social media.

A companion survivor resource is included with this booklet that can be given directly to survivors. In addition, on page 18 of this booklet, there is a link to a one-page multi-lingual resource that your organization can provide directly to survivors. To ensure that this booklet is accessible to individuals at all levels of technological know-how, a glossary of basic terminology is included on page 19. If you are unfamiliar with current technology, or simply need a refresher, please review the glossary before reading this booklet. Every glossary term is hyperlinked the first time that it appears in the document. If you click on the term, it will automatically take you to the definition. For instance, if you click on the term "social media" above, it will take you directly to the definition in the glossary. ***If you experience trouble accessing any links, please copy and paste the URL into your browser and click "enter."***

Helping Survivors with Personal Privacy Management: Advocacy Checklist

Use this checklist in your advocacy or counseling sessions with survivors to be sure you have covered the relevant privacy and safety issues in this information booklet.

What Information Should I Cover with the Survivor?

Not all of the information contained in this booklet is relevant to all survivors. Before covering this information in detail with a survivor, consider the questions below. The answer to these questions will help you decide how much of the information contained in this booklet you need to discuss with the survivor. For instance, if the survivor is involved in a court case, he or she needs to be aware of how the information contained on social media may come to light as part of that court case. If the survivor is in crisis, then discussing this booklet may not be important at the moment, unless the victimization involves Internet or social media stalking or harassment.

- Is this a recent assault/situation?
- Does the survivor want to pursue criminal charges?
- Does the survivor use social media/technology, and if so how?
- What is the survivor's relationship to the perpetrator?
- Have there been any instances of stalking or sexual harassment?
- Is the survivor connected to the perpetrator in any way on social media?

Help Survivors Manage Their Accessible Information

- ☐ Encourage survivors to set social media privacy settings
- ☐ Have survivors test and review social media privacy settings
- ☐ Caution survivors about information shared by family and friends
- ☐ Warn survivors about technology that can identify location
  Geo-Tagging
  Location "Check-In" Applications
  GPS
- ☐ Explain to survivors how to protect personal information (name, address, phone number)
- ☐ Encourage survivors to change passwords

Educate Survivors About Enhancing Privacy on Portable Electronic Devices

- ☐ Warn survivors about GPS technology
- ☐ Educate survivors about spyware

Teach Survivors About Protecting Against Future Problems

- ☐ Teach survivors how to document communications

TABLE OF CONTENTS

TEACH SURVIVORS SAFER WAYS TO USE TECHNOLOGY

Encourage Survivors to *Set and Recheck* Social Media Privacy Settings

Every social media site, such as Facebook, MySpace, LinkedIn, Google+, and Twitter, provides users with the ability to set limitations on the public's ability to access their information. These are known as privacy settings. Privacy settings are essential to protecting personal identifying information. Unfortunately, adjusting privacy settings on social media sites can be complicated and time-consuming. Keeping up with changes to privacy policies on various social media networks also presents an ongoing challenge. Privacy settings must be regularly monitored to keep up with the ever-changing structure of social media sites. For example, when Facebook launched the Timeline feature in February 2012, content posted by users before privacy features were available on Facebook automatically defaulted to public view.

The first step for assisting survivors with privacy settings is to ask survivors to think about who they want to have access to their information. Survivors should be encouraged to think critically about how their information – and their child's or family member's information – is currently being shared, and how they would like their information to be shared in the future. Ask survivors specific questions about how their information is currently shared:

- Who is in their network on Facebook? LinkedIn?
- Who follows them on Twitter? Foursquare? Photo-sharing sites?
- What about the networks and/or followers of their children or family members?
- Is the survivor, or the survivor's children or family members, connected to the perpetrator on social media?
- Is the survivor connected to someone (friends, family, or coworkers) on social media who is also connected to the perpetrator?
- Does the survivor's profile allow people to search for the survivor?
- Is the information posted on their page available to
    - the public?
    - their network?
    - their extended network?
- In cases of domestic violence or child sexual assault, would changing the way that the survivor's friends and family share information alert the perpetrator to the survivor's plans to escape, placing the survivor or the survivor's children at risk of harm?

After these questions are answered for each social media service the survivor uses, the survivor is ready to adjust her or his privacy settings. **It is a best practice for advocates to alert survivors to regularly monitor and update privacy settings for their own as well as their child's accounts because options for privacy settings are subject to change without notice from the social media service.** Privacy settings and controls vary for each social networking site, so it is helpful for survivors to visit each site they use and explore the privacy options. To access privacy settings on a social media account, a survivor can sign into her or his account and click on "account settings" or a similar link. Social media sites typically provide information about privacy settings in their "Help" sections, and some sites even offer tutorials for selecting privacy settings:

Facebook: http://www.facebook.com/help/?page=132569486817869
MySpace: http://www.myspace.com/pages/privacysettings
Twitter: http://support.twitter.com/articles/14016
Foursquare: https://foursquare.com/privacy/
LinkedIn: http://learn.linkedin.com/settings/

While every social media site has different privacy settings, the following tips offer guidance for adjusting privacy **on Facebook** to give survivors a starting point for managing their online information. Advise the survivor to:

- **Enable Secure Browsing (https)**

  HTTPS browsing uses codes to provide increased security and privacy. An https connection offers the same type of secure connection used by banks and shopping sites. Enabling secure browsing will make the social media site slightly slower, but will make it extremely difficult for anyone to hack into the account. **To enable secure browsing, check the https box under "Account Security."**

- **Disable "Check-In" Application**

  By default, Facebook allows "friends" to tag and "check in" other users, revealing their exact location. If the user wants to remain in control over location tracking, she or he must disable "friend tags" or "check-in" capabilities in the privacy settings.

  See http://www.facebook.com/about/location for more information about Facebook's "Check-In" applications.

- **Disable "Instant Personalization"**

  Instant personalization allows third parties (like shopping sites) to access a user's personal data in order to "personalize" the user's web browsing. A survivor can opt out of this personalization by leaving the checkbox ("Enable instant personalization on partner websites") unchecked.

- **Disable "Public Search"**

  When people search for a user's name on a search engine (such as Google), they may get a glimpse of the user's personal information. Inform the survivor to uncheck the "public search" checkbox to disable this feature.

- **Limit Information Sharing**

  Each type of information – photos, comments, status updates, personal bio information, relationship status, etc. – can be limited to "everyone," "friends of friends," "friends," or "only me." For optimal protection, encourage survivors to select "friends" or "only me" to keep their information within their network of accepted friends. For information like comments and wall posts, a survivor may want to limit sharing to "only me" to prevent her or his personal information from being shared by a friend or family in a post or comment on another page.

  If users are not careful, third parties can still access information through their network of friends or followers if these others' privacy settings are not as strict. The survivor can modify the "info through friends" setting to prevent inadvertent sharing through friends.

- **Create and Monitor "Friend Lists"**

  Creating "friend lists" allows a user to specify the content visible to each list of friends. This would allow a survivor to limit the content available to a perpetrator, or friends of a perpetrator, without blocking their access completely. This may be an essential safety tool for a survivor who is still in a relationship, or is attempting to leave.

Encourage Survivors to *Test and Review* Social Media Privacy Settings

To be sure the privacy settings are providing the appropriate level of protection, survivors can:

- Search for their page and the pages of their children and other family members on the social media site itself (without logging in). Also search on Google or on another search engine, to see what content is available to the public.
- Ask a friend or family member who *is not* in their social media network to access their page and attempt to post, tag, or comment.
- Ask a friend or family member who *is* in their social media network to access their page and attempt to post, tag, or comment.

Remember: **privacy settings are not perfect**. Even private information posted on a social networking account may still be discoverable in a legal proceeding, such as

custody or divorce, and may be introduced as evidence in civil or criminal proceedings. Privacy settings – like all technology – are subject to error and may not always work perfectly to protect an individual's information. **Encourage survivors to review the content of old posts and think about potential consequences before posting any new content. Explain to survivors that even when deleted, information (including emails, pictures, status updates, etc.) posted online never really goes away**

The following resources provide more information about privacy considerations for online content:

- The National Network to End Domestic Violence SafetyNet Project, *Privacy Considerations When Posting Content Online*, *available at* http://www.nnedv.org/docs/SafetyNet/OVW/NNEDV_PostingContentOnline.pdf
- National Resource Center on Domestic Violence & National Sexual Violence Resource Center, Special Collection: Technology Safety and Advocacy (2006), *available at* http://vawnet.org/special-collections/TechSafety.php
- National Sexual Violence Resource Center, Internet Safety Online Resource Collection, *available at* http://www.nsvrc.org/projects/internet-safety-online-resource-collection
- Privacy Rights Clearinghouse, *Fact Sheet 35: Social Networking Privacy – How to be Safe, Secure, and Social*, *available at* http://www.privacyrights.org/social-networking-privacy

Caution Survivors About Information Shared by Family and Friends

Even with strong privacy settings, careful attention to information disclosure, and limited content sharing, a survivor's family and friends might still share personally identifying information without the survivor's knowledge. While this type of disclosure may be inadvertent, the risk is still enormous.

It is important to encourage survivors to talk with friends and family members about the importance of their privacy. Suggest that they ask family and friends to refrain from posting pictures, comments, and other information about them that may reveal location or other identifying information.

On Facebook, there are a few ways to **minimize inadvertent disclosure by family and friends** by setting restrictions on content. Survivors can change Facebook settings to:

- Require their approval prior to allowing friends to tag photos or post comments to your wall.

- Disable “check-in” capabilities to prevent friends and family from revealing their current location.
- Restrict the ability for their Facebook “friends” to see comments posted by others by selecting “only me.”

Again, these measures will offer a survivor some, but not absolute, protection. Stress to survivors that talking to friends and family, particularly teenage children, about the importance of privacy is key to shielding against unwanted disclosures of personal information.

SafetyNet, a project of the National Network to End Domestic Violence, has a helpful resource that advocates can provide to survivors to share with their children, *Tech Savvy Teens: Choosing Who Gets to See Your Info*. It is available at: http://www.nnedv.org/docs/SafetyNet/NNEDV_TechSavvyTeens_English.pdf

Warn Survivors About Technology That Can Identify Location

Geo-Tagging

Geo-tagging is the process of embedding an image or electronic communication with the geographical location where the image or communication came from. For instance, if a survivor takes a picture with her or his phone or digital camera, the picture will have geographical coordinates (longitude and latitude) embedded in the photo file that pinpoints the exact location where the photo was taken. Other information, such as the time and date that the photo was taken, is also embedded in the photo file. When a geo-tagged photo or communication is posted to the Internet, anyone with a little technical know-how can access the exact location, time, and date that the photo or communication was taken. In fact, many social networking sites are designed to extract the information and post the location, date, and time automatically. For instance, Facebook’s Timeline feature is designed to extract geo-tag information from photos, videos, posts, status updates, and other communications to create a literal map of the user’s life.

If a survivor, or the survivor’s children or family members, unknowingly posts images or communications with geo-tags, a perpetrator may be able to track them to a confidential location. And, because the geo-tag also contains time and date-stamp information, a posted image may reveal when the survivor is home or away – putting her or him in danger of being stalked, harassed, or physically endangered. While this danger is most relevant to social media because a majority of photo sharing takes place in that forum, keep in mind that geo-tags are embedded in all photos. So, for instance, photos of items for sale posted to craigslist® or eBay® and photos of a child’s field trip or sporting event posted to a school website may also contain geo-tag information.

The danger to a survivor may be avoided by removing the geo-tag before posting the photo or communication online. The survivor should be encouraged to check the owner's manual for their camera, phone, or other electronic device to learn how to turn off the geo-tagging feature. If relevant to the survivor, she or he should also check the settings on their children's camera, phone, or device – especially if the child received the device as a gift from the perpetrator. Survivors should also be advised to request that their friends and family remove geo-tags before posting images or communications that reference the survivor or their children. In addition, survivors should be advised to withhold permission from schools, sports teams, and other youth organizations that may want to publish photos of the children on social media or other websites.

If the survivor has an **iPhone**, you can give these instructions for how to turn off geo-tagging: Go to "settings," and click on "general" and on "location services." Select "camera" and turn off the camera's location services. This will turn off the geo-tagging for pictures taken with an iPhone, but remind the survivor that other activities online and on social media may still reveal location.

Location "Check-In" Applications

There are several social networking applications and programs available today that allow users to "check in" to the places they visit. The technology pulls information from GPS on the individual's phone or other portable electronic device and pinpoints the location on a map. Foursquare, for example, is a popular application that uses this technology. Foursquare allows users to "check in" to a location, and have that information simultaneously appear as a status update on their Twitter and Facebook accounts. Foursquare matches the user's location to coupons and other deals at nearby locations. This is a way to stay connected with friends, but also works as a tool for perpetrators to keep tabs on a survivor's every move.

"Check-in" applications are particularly dangerous because they may be connected to a survivor's social networking sites without the survivor's knowledge. If a survivor's "check-in" application is not disabled, a friend or acquaintance could "check in" the survivor, or could "check in" on their own and indicate that they are with the survivor – all without the survivor's knowledge. For instance, a coworker could "check in" at a restaurant on Foursquare and could list all the names of the people who are dining together. If the survivor is connected with the coworker on social media, the survivor's name would be automatically highlighted with a hyperlink, and the survivor's location at that restaurant would appear on her or his social media page as a status update.

Be sure to advise survivors to check their privacy settings and turn off any location "check-in" applications. Also, they should make certain that their privacy settings prohibit others from checking them in at locations without their explicit approval. *See page 4, Encourage Survivors to Set and Recheck Social Media Privacy Settings.*

GPS

GPS technology is installed in most portable electronic devices on the market today, including phones, tablet computers, personal planning devices, iPods, etc. The GPS feature may be turned on without the user's knowledge, and could be used to pinpoint the user's exact location.

For an in-depth examination of GPS, and tips for safety planning, see page 13, Inform Survivors About How to Enhance their Privacy on Portable Electronic Devices: Warn Survivors About GPS Technology.

Explain to Survivors How to Protect Personal Information

(Name, Address, Phone Number)

Data brokers pose a distinct risk to a survivor who is attempting to shield her or his location and/or identity to avoid being located by a perpetrator. Each time a survivor signs up for special deals or essential services, she or he is asked to provide the company with personal information – name, address, date of birth, phone number, etc. Sometimes providing this information is optional, but usually the information is required. Data brokers purchase this personal information and store it in large, searchable databases. Some charge a fee for accessing the database, but others provide free access. See, for instance, http://www.zabasearch.com or http://www.spokeo.com. These sites offer free access to basic personal information, such as an individual's address. For an additional small fee (approximately $2.95-$12.95), the sites provide detailed profiles of individuals, including the person's email address, phone number, income information, and family member information. Some data brokers are now gathering additional information, such as medical conditions, residential or tenant history, check-writing history, employment background, driving history, and insurance claims. These types of data brokers can pose a serious threat to a survivor who is trying to rent an apartment and/or gain financial independence from a perpetrator.

It is unrealistic to expect survivors to refrain from accessing services that require information disclosure. And, unfortunately, it is extremely difficult – if not impossible – to prevent data brokers from collecting an individual's personal information. However, survivors should be aware of this dangerous technology so that they are aware of the threat and can mitigate the harm that may come from disclosing such information.

Most stores require only a name or – at most – an email account to obtain a store credit or discount card. However, even when it is necessary for individuals to share their personally identifying information, **there is typically a mechanism – either a checkbox, a call-in number, or a mail-in card – that allows individuals to protect their personal information from being disclosed to a third party**. For instance, electricity suppliers are required by law to allow anyone to protect personal information from being disclosed to electricity marketers. Electric companies send a mailer card in

each customer's bill, or sometimes in a separate mailing, that allows customers to "opt-out" of disclosing personal information. Electric customers may also call the company directly to be taken off the marketing list.

There are a few steps that survivors can take to reduce the threat posed by data brokers:

- Set up a dummy email account to use for any special offers or services.
- Do not include any information that is not essential for enrollment in the offer or service.
- Whenever possible, "opt-out" of information disclosure by checking a box, calling a number, or returning a mailer card.

The following resources offer additional information about data brokers and provide suggestions for reducing harmful results:

- Privacy Rights Clearinghouse, Online Information Broker FAQ, http://www.privacyrights.org/online-info-broker-faq
- Privacy Rights Clearinghouse, Online Information Brokers and Your Privacy, http://www.privacyrights.org/ar/infobrokers.htm
- Privacy Rights Clearinghouse, Fact Sheet: "Other" Consumer Reports – What You Should Know About "Specialty" Reports, http://www.privacyrights.org/fs/fs6b-SpecReports.htm

Encourage Survivors to Change Passwords

While choosing a strong and secure password is important for every individual, it is particularly important for survivors of domestic and sexual violence. The most common passwords that people use contain personal data, such as family names and birthdates. An anonymous hacker is not privy to such personal information, but those who know the survivor well are privy to a survivor's personal information because they have lived with or known the survivor for a long time. If a perpetrator has access to a survivor's account, he or she can maintain control over a survivor long after separation. Access to a survivor's online accounts would allow a perpetrator to disrupt automatic payments, send fake emails or other messages that destroy the survivor's reputation, access bank accounts, discover a survivor's confidential location, or shut off essential services such as electric and gas.

Given the extreme risk facing survivors, advocates should advise all survivors to carefully select passwords for every online account. Online accounts include banking or credit accounts, social media, email, shopping accounts such as Amazon® or eBay®, and other sites with secure login. Different passwords should be used for every online account, and survivors should be encouraged to choose security questions that are not

easily guessed by the perpetrator. Survivors should also be advised to ask children, family, and close friends to select secure passwords and security questions.

It is extremely important for survivors to create new passwords using a secure computer or electronic device. If the computer or device is monitored through the use of spyware, any data entered on that computer or device is transmitted to the spyware user. So, if a computer or other electronic device is infected with spyware, it will not matter whether the survivor chooses a secure password because the person who installed the spyware will be able to see the new account login and password. *For more information on spyware, see page 14.*

Here are 5 tips that you can review with survivors for creating a password that is easy to remember, but hard to crack:

(1) **Do not use personal information,** like names or birthdates of friends, family, or pets or social security numbers.

(2) **Create passwords that use a minimum of 10 characters,** mixing in capital letters, punctuation, numbers, and other characters.

(3) **Insert characters or numbers in place of similar letters.**

- "social media" becomes "$oci@1 m3di@"

(4) **Try using the first letter of each word in a sentence that is easy to remember, or use a series of words strung together with punctuation.** These are known as "passphrases."

- "I am doing this for me" becomes "I@DT4M."
- "I_@m_$trong.

(5) **Create new passwords on a computer or device that is not accessible to the perpetrator**, like work computer or a friend's computer.

- *A library computer or other public computer may pose other safety risks. When on a particular website, look to see if the URL contains the first letters "https." The "s" indicates that the website is secure. Also, be sure to delete cookies, browser history and other information that is collected and stored during your browsing session.*
  - For illustrated instructions on how to delete this information from popular web browsers, *see* PCWorld, *How to Delete Cookies* (2011), *available at* http://www.pcworld.com/article/242939/how_to_delete_cookies.html

INFORM SURVIVORS ABOUT HOW TO ENHANCE PRIVACY ON PORTABLE ELECTRONIC DEVICES

Warn Survivors About GPS Technology

Almost every phone and many types of portable electronic devices (such as tablet computers) have GPS capabilities that, when turned on, can pinpoint the user's exact location just about anywhere in the world.

A perpetrator may hide a GPS device on a survivor's phone or in a survivor's vehicle, or may access the survivor's GPS-enabled devices electronically. Unfortunately, technology on the market today allows third parties to use the GPS capability to remotely monitor the user's location by installing a simple, undetectable program onto the phone or device. The third party does not even need to have physical access to the phone or device to install the program – installation can be accomplished remotely with just a little technological know-how. For survivors, this means that their movements may be tracked without their knowledge, enabling perpetrators to maintain power and control by having intimate knowledge of their whereabouts at all times.

It may not be readily apparent whether the survivor is being tracked through GPS. When counseling a survivor, ask about unusual or unexplained behavior. Is the perpetrator showing up at odd locations, such as a stoplight, supermarket, or doctor's office? Does the perpetrator always seem to easily locate the survivor, even when the survivor has not told anyone about her or his plans? These types of behaviors are a good indication that the perpetrator is using GPS to track the survivor's exact location.

Review the following tips with survivors to minimize their risk of being tracked through GPS-enabled devices:

- **Keep phones off as much as possible.**
    - Remote installation of tracking programs is typically accomplished by calling a phone for approximately 30 seconds. The targeted person does not even need to answer the phone. But, if the phone is off, the software cannot be installed. Thus, if the survivor keeps their phone off as often as possible, the threat is significantly reduced.
- **Take the battery out of the phone or electronic device when not in use.**
    - Many GPS-enabled devices continue to track locations, even when the phone is off. If a phone has GPS capability, the only way to disable it for sure is to remove the battery.

- **Never leave phones or other electronic devices unattended.**
  - Even though many programs now allow for remote installation, cheaper versions still require physical access to the device in order to complete installation. However, it only takes a few moments to install monitoring software on a phone, therefore, survivors should be counseled to maintain control of their phones at all times.
- **Check with mobile phone service providers to see if the survivor's account includes GPS monitoring.**
- **Purchase a new phone or use a donated phone as a primary phone.**
  - If a survivor wants or needs to maintain contact with their perpetrator, encourage her or him to purchase a new phone (such as a pay-as-you-go phone) or use a HopeLine phone to communicate with family and friends, and use the old phone for communications with the perpetrator. This way, the phone that is regularly used to communicate with supportive friends and family will be less at risk of being tracked or having spyware installed.
    - For more about Verizon Wireless HopeLine Program, see http://aboutus.verizonwireless.com/communityservice/hopeLine.html
  - Advise survivors to manually transfer their contacts into the new phone. Information from the survivor's old phone should never be transferred electronically to the new phone because that type of transfer will also transfer spyware and other malicious software or programs.
- **Have the survivor's vehicle checked by a new mechanic to remove or disable GPS-enabled devices.**
  - Safety-plan with the survivor before suggesting this step to identify any safety risks that may come from the perpetrator realizing the GPS device was found. Also, it may be best to involve law enforcement before taking this step if the survivor wishes to pursue any type of criminal or civil action.

Educate Survivors About Spyware

Spyware can be installed on a smart phone or a computer. This type of software typically requires physical access to the device in order to be installed, but new technology also allows for remote installation, as do GPS tracking programs. Spyware allows a third party to access files and to track and monitor all online and offline activities.

Discuss these tips with survivors for keeping electronic devices safe:

- **Install and regularly update anti-virus, anti-spyware, and anti-malware software**

- Advise survivors to run anti-virus, anti-malware, and anti-spyware software on their computers. The software should be regularly updated to keep up with changing technology.

- **Scan computers regularly**
  - Survivors should also conduct regular computer scans to catch any spyware that may have evaded the anti-virus, anti-malware, and anti-spyware software. Bitdefender is a free online scanner: http://www.bitdefender.com/scanner/online/free.html

- **Access the Internet from a safer computer**
  - If a survivor's computer is being monitored, everything will be recorded. Counsel survivors to access the Internet for research and safety planning activities from a safer computer, such as a library or other public computer. It is essential, however, to also advise survivors to continue using their personal computer to avoid raising the perpetrator's suspicion.
  - *Accessing the Internet from a public computer is not always safe*. Advise survivors against accessing financially sensitive information, such as bank accounts, credit cards, and bill statements, on public computers. If the survivor must use a public computer for these purposes, be sure to inform survivors about how to delete cookies, stored passwords, and browsing history after using the computer to protect against identity theft or other general safety risks.
  - For *illustrated* instructions on how to delete this information from popular web browsers, *see* PCWorld, *How to Delete Cookies* (2011), *available at* http://www.pcworld.com/article/242939/how_to_delete_cookies.html

For more information on spyware, including information on how the technology works and tips for survivors and their children, parents, and friends and family, see *Who's Spying on Your Computer?*, *available at* http://www.nnedv.org/docs/SafetyNet/NNEDV_SpyWareAndSafety_English.pdf a resource produced by SafetyNet, a project of the National Network to End Domestic Violence. This resource is also available in Spanish.

HELP SURVIVORS PROTECT AGAINST FUTURE PROBLEMS

Teach Survivors How to Document Online Communications

Survivors should be advised to keep close records of any threatening communications, including communications on social media, through text messages, or via email. While many electronic communications can be traced even if they are later deleted, the process for recovering a deleted message can be very difficult and expensive. To preserve evidence for future litigation, the survivor can print a copy, save the email, photo, page, or file to a safer device, and/or take an actual photograph of the screen. Here are some specific ways to advise survivors to document different types of communication:

- **Text Messages**
  - The survivor can take a picture of the phone with the text messages displayed, as well as a picture of the messages and the survivor's response (if any). The survivor should print the picture and store it in a safe place.
  - Also, the survivor can re-type the text messages into a word document, and print a hard copy.
- **Email**
  - Survivors can save and print a copy of the email, making sure to include the full header that includes the date, time, and original sender of the email.
    - The website http://www.cyberbullying.info/resources/headers.php has more information on how to view and print a full email header.
  - Also, if the survivor begins to receive emails that disappear from her or his inbox immediately upon reading, advise the survivor to take a picture of the screen with a camera for all future emails.
- **Social Media**
  - The survivor can print out the web page, making sure the date and time of the post is included and is legible in the printout.
  - If the survivor's computer will not directly print the social media page, the survivor can save and print a picture ("screen-shot") of the social media

site, making sure the message or post is visible in the picture, along with the date and time that the message or post was sent.

If the survivor does not know how to take a screen shot, you can review these instructions together:

- For a Mac:
  - Hold down Command+Shift+4 and hit the spacebar.
  - Click on the screen you want to capture in a photo.
  - The photo will save automatically to your desktop.
- For a PC:
  - Press the Print Screen key (PrtScn).
  - Open an image-editing program, such as Microsoft Paint.
  - Go to the Edit menu and choose Paste.
  - Go to File menu and choose Save As.

Saving a copy of the communication to a computer file may not be advisable. If the perpetrator has installed spyware on the survivor's computer or other electronic device, he or she may be able to delete any files saved on that computer. The survivor should be advised to print a hard copy of any communications and keep the copies in a safe place in case of an emergency.

ADDITIONAL ADVOCACY RESOURCES

- NNEDV, SafetyNet, *Technology Safety Planning with Survivors*, *available at* http://www.nnedv.org/docs/SafetyNet/NNEDV_TechSafetyPlan_English.pdf
    - *This resource is a one-page tip sheet that can be distributed to survivors to help them plan for their online safety. It is available in eight languages - English, Spanish, Chinese, Korean, Vietnamese, Somali, Russian, and French.*
- National Resource Center on Domestic Violence & National Sexual Violence Resource Center, Special Collection: Technology Safety and Advocacy (2006), *available at* http://vawnet.org/special-collections/TechSafety.php
- National Sexual Violence Resource Center, Internet Safety Online Resource Collection, *available at* http://www.nsvrc.org/projects/internet-safety-online-resource-collection

GLOSSARY OF BASIC TERMINOLOGY

"Check-In" Application

"Check-In" applications allow social media users to share where they have been, where they are now, and where they are going. When a person "checks in," a post or status update will show on the web or social media site so others will see where the person is. When a check-in application is enabled, it tracks the user's location through the GPS in the user's phone or other electronic device.

There are many stand-alone "check-in" applications available on the market (most of them free) and many popular social networking sites also use the technology. Here are links to some of the more popular check-in applications and sites for you to share with survivors:

- **Facebook**: http://www.facebook.com/about/location
- **Foursquare**: https://foursquare.com/
- **Loopt**: https://www.loopt.com/
- **Yelp**: http://www.yelp.com
- **Gowalla**: http://gowalla.com/

Cookies

Many websites deposit data about a user's visit, called "cookies," on the hard drive of the user's computer. Cookies are pieces of information sent by a web server to a user's browser. Cookies may include information such as login or registration identification, user preferences, online "shopping cart" information, and so on. The browser saves the information and sends it back to the web server whenever the browser returns to the web site. The web server may use the cookie to customize the display it sends to the user, or it may keep track of the different pages within the site that the user accesses.

Information excerpted from Privacy Rights Clearinghouse, *Fact Sheet 18: Online Privacy, Using the Internet Safely* (2012), http://www.privacyrights.org/fs/fs18-cyb.htm

Data Brokers

A growing number of websites sell (or give freely) the personal information of individuals. These online information brokers (also known as *data brokers* or *data vendors*) gather personal information from many sources including white pages listings (directory assistance), publicly-available sources and public records. Some information brokers also offer the ability to conduct "social searches," which gather information by searching public profiles on social networking sites.

Information excerpted from Privacy Rights Clearinghouse, *Online Information Brokers and Your Privacy* (2012), http://www.privacyrights.org/ar/infobrokers.htm

Embedding

Essentially, when an image or other form of media is "embedded," it means that information the user cannot see is added to the file that contains the image or other media. This type of information is commonly known as metadata. In relation to geo-tagging, embedding means that location-based metadata is added to the file, allowing the computer – and anyone with a little technological know-how – to see the location where the file originated. For instance, when a survivor takes a picture at a friend's house, metadata about the survivor's location when the picture was taken is added to the picture file. Later, when the user loads the picture to a computer, the computer is able to "see" where that picture was taken.

"Friend"

A "friend" on social media is someone that a user allows to be in her or his network (see definition of network). Most social media sites allow users to connect to one another by sending and confirming "friend" requests. After the user accepts a friend request, the two users are "friends" and are part of each other's networks.

Social Media

The Merriam-Webster Dictionary defines social media as "forms of electronic communication through which users create online communities to share information, ideas, personal messages, and other content." The definition of social media continues to evolve, but for the purpose of this booklet, references to social media include any website that allows users to exchange information, ideas, and content.

**See* MERRIAM-WEBSTER DICTIONARY ONLINE, SOCIAL MEDIA, www.merriamwebster.com.

Network

A network, for the purpose of this booklet, is the group of people who are connected to an individual through a social media website. Anyone who has the ability to connect to the user is in that user's network, even if privacy settings are set to limit the other's ability to see some of the user's content.

Secure Browsing (https)

HTTPS, or secure browsing, means that data transferred by the website is encrypted so that it cannot be read by anyone except the recipient. HTTPS browsing is used by websites that collect sensitive data, such as financial information. A user can tell when a page is using HTTPS browsing in two ways:

1. There may be a lock icon in the browser windowpane where the URL is displayed.
2. The URL will contain "https://" at the start.

**Information excerpted from* http://webdesign.about.com/od/http/g/bldefhttps.htm

For more definitions, see SOCIAL BRITE, SOCIAL MEDIA GLOSSARY: THE TOP 100 WORDS & PHRASES IN THE SOCIAL MEDIA DICTIONARY, http://www.socialbrite.org/sharing-center/glossary/