How to Gather Technology Abuse Evidence for Court

SELF-REPRESENTED LITIGANTS SERIES

Authors: Kaofeng Lee, Deputy Director, and Ian Harris, Technology Safety Legal Manager, the Safety Net Project at the National Network to End Domestic Violence (NNEDV). Website: https://nnedv.org/content/safety-net/.

If someone is using technology like text messages, email, or social media (like Facebook) to harass you, this guide will help you "capture" the evidence of the harassment, so you can bring it to court. You might think you can just show the judge your phone in court—but you probably won't be allowed to just show your device. Even if you are allowed, you could risk the court taking your device as evidence. To be sure the judge considers your evidence and that you don't lose your phone (or other device), you need to gather evidence in a form allowed by the court. This guide will provide suggestions on how to capture evidence that can be admitted in court from your devices, such as your cell phone, computer, or tablet (such as an iPad).

This quick guide has links to websites and some national telephone numbers that may help you. If you need help capturing a piece of evidence we do not discuss in this guide, please call our confidential toll-free number, **1-800-527-3223**. We can also provide information about local and national resources related to domestic violence and child custody. We can refer you to help close to you or mail you information packets that might be helpful. You can also download many of these informational resources from our website at **www.rcdvcpc.org**.

For more help, visit the website or call anytime.

NCJFCJ
est. 1937
NATIONAL COUNCIL OF
JUVENILE AND FAMILY COURT JUDGES
WWW.NCJFCJ.ORG

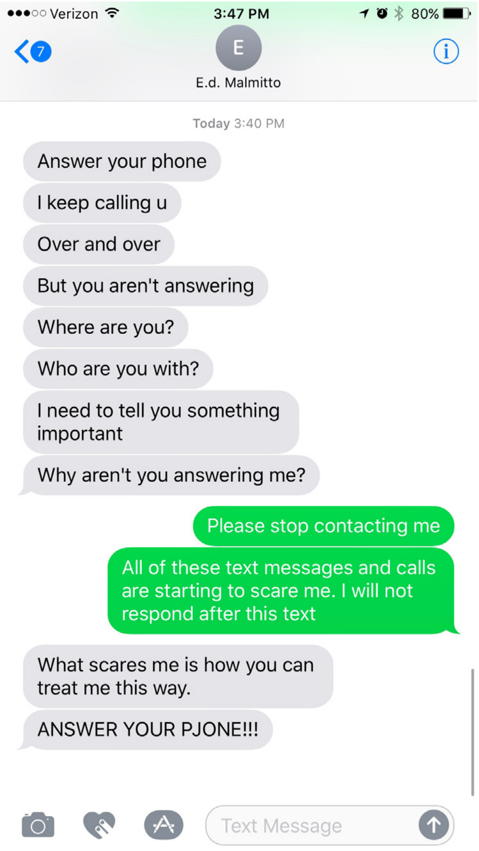
CELEBRATING 80 YEARS 1937-2017

RCDV:CPC
Resource Center on Domestic Violence:
Child Protection and Custody

Capture the Message

Take a screenshot

Most phones, computers, and tablets allow you take a picture of whatever is on the screen. This is called a "screenshot." A screenshot will only capture what you can see on your screen, so you may have to take multiple screenshots to capture everything. For example, you will generally need to take multiple screenshots to capture a text messages conversation:



Today 3:40 PM

Answer your phone

I keep calling u

Over and over

But you aren't answering

Where are you?

Who are you with?

I need to tell you something important

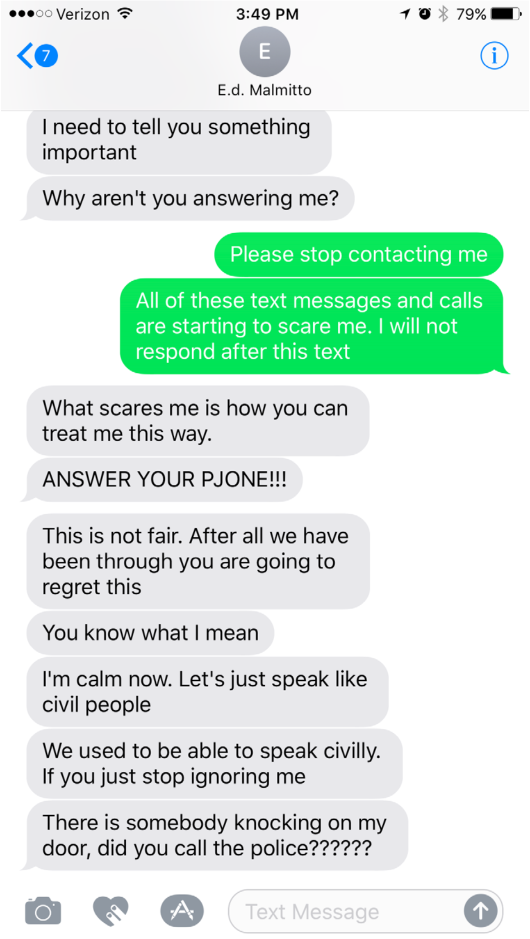
Why aren't you answering me?

Please stop contacting me

All of these text messages and calls are starting to scare me. I will not respond after this text

What scares me is how you can treat me this way.

ANSWER YOUR PJONE!!!



I need to tell you something important

Why aren't you answering me?

Please stop contacting me

All of these text messages and calls are starting to scare me. I will not respond after this text

What scares me is how you can treat me this way.

ANSWER YOUR PJONE!!!

This is not fair. After all we have been through you are going to regret this

You know what I mean

I'm calm now. Let's just speak like civil people

We used to be able to speak civilly. If you just stop ignoring me

There is somebody knocking on my door, did you call the police??????

Also, please be aware that some apps, like Snapchat, will notify the sender of a post you take a screenshot of, which may not be safe for you. See the section below on Snapchat for suggestions on how it may be possible to avoid this problem. (This isn't a problem for text messages and other apps like Instagram, Facebook, and Twitter, which don't notify the sender when you take a screenshot.)

HOW TO TAKE A SCREENSHOT

Taking a screenshot can be slightly different for each device, but you can watch this video to see generally how to take a screenshot on a computer or a smartphone: http://techsafety.org/resources-survivor/screenshot-videos. You can also do an online search for "How to take a screenshot on a [your specific phone or tablet]" for instructions on how to take a screenshot on your device.

Device	Take a screenshot	Find the screenshot
Windows laptop or computer	Find the key on the keyboard that says: PrtScn, Prt Scr, or Print Screen	Immediately after taking the screenshot, open a document that lets you paste an image (such as Word or Google Docs), and "paste" the screenshot.
Mac laptop or computer	At the same time, press these keys: Shift + Command + 3. This will save the screenshot onto your computer desktop.	Screenshot will be saved onto the desktop as a picture.
iPhone or iPad	At the same time, press the On/Off button + the Home button. For iPhone X, press the On/Off button + the Up Volume button.	Screenshot will be saved into your Photos app as a picture.
Android phone or tablet	Android devices differ. You should try the following options: 1) Down Volume button + Home button, 2) On/Off button + Home button. If neither of those work, try an online search for "How to take a screenshot on a [your specific phone or tablet]"	Screenshot will be saved into your Gallery as a picture.

PRINT THE SCREENSHOT

You can paste your screenshot (or picture) into a document using a program that lets you paste an image (like Word, Pages, or Google Docs). Print the document that includes the screenshot. You may also want to email or text message the document to a device that you will continue to have secure access to, so that you have an extra copy.

Take a photo

If your phone or computer doesn't allow you to take a screenshot, take a photo of the computer, phone, or tablet screen with another camera. (This can also be a way to avoid the problem with Snapchat and similar apps that notify the sender when you take a screenshot—see more below under Snapchat.) Be sure to capture the message and the entire screen. Sometimes, the screen can be quite small, so you may want to make sure you hold the camera close. Look at the photo to make sure that the words are easy to read and any image is clear.

PRINT THE PHOTO

If you took a photo, you can print it as you would normally print other photos. If you have a digital photo, you could copy or "insert" the photos into a document and print the document. Just make sure that any image is clear and any words are easy to read.

Record a Video

You can also take a video of the message. This might be helpful if you have a lot of information you want to capture and taking photos or screenshots is too slow. (This can also be another way to avoid the problem with Snapchat and similar apps that notify the sender when you take a screenshot—see more below under Snapchat.) Be sure to hold your camera steady while you scroll through the content you want to document.

For computers, there is screen capture software that can record what you see and do on the computer. This is similar to a screenshot, but instead of taking photos, it creates a video of what you do on the computer. Some of the free software you can download to your computer are: CamStudio, ezvid, and Icecream Screen Recorder. Similar software may be available for your phone as a built-in app or an app you can download, but please be aware that for Snapchat and similar apps, these apps may notify the sender that you recorded the post, which could be dangerous for you. See more information below under Snapchat.

Check to make sure that the court can

play the video. You can print a photo or a screenshot, but a video will need to be played on a video player. Talk to the court (or your attorney or an advocate if you are working with one) to see if they can accept a video as evidence. If so, ask what type of video file the court can play. Videos can be recorded in different format types, and only certain media players can play certain files. If the court cannot play your video format, there are free video format converters online. Just search online for “free video format converter from [your device or video format] to [video format accepted by the court].” If the court can play a video, and you have converted the video into a format that the court can accept, then save the video file onto a CD, DVD, or flash drive. Ask the court if they need or prefer a particular storage type—some courts may not accept a flash drive, for example. The court will keep the DVD, CD or flash drive in the court file after you introduce the evidence. Let the court know in advance that you will be presenting evidence this way because most courts will not just allow you to play your device, such as your phone, in court.

Make an Audio Recording

If you want to capture a voicemail message, you can do that with an audio recorder app on your phone or a traditional tape recorder. Again, check with your local court to see how you can play a recorded audio file. If the court can play your audio recording, save the audio recording onto a CD or DVD. (Again, you will not be allowed just to play your phone in court!)

IMPORTANT: Depending on the state you live in, it may be a crime to record a phone conversation without the permission of everyone who is participating in the conversation. If you want to record a phone conversation between you and another person, talk to a lawyer first. Although you can find some information online, laws can change quickly, so it is best to talk to a lawyer.

KEEP IT SAFE

Once you’ve captured your message, it’s important that you save it somewhere safe: somewhere you won’t lose it or someone else won’t have access to it. For example, you may not want to save evidence onto a phone, computer, or tablet that the abusive person has access to. Even if you do not think they have access, you may still want to change passwords and put in other security measures.

IMPORTANT: Your safety is important, too. If you think the other person might become more abusive if your evidence is discovered, consider asking a friend to capture the message on their own phone or computer and share it with you. However, make sure the friend knows that capturing the evidence could mean that they have to go to court to testify for your case.

Tell the Story

When you are capturing evidence to explain to the court what is happening, you may need to show more than just one message. Courts often want to see entire conversations, so might need to capture many messages to tell the whole story. You will also want to capture additional information about the person sending you those messages.

Capture More Than One Message

It is important that you capture entire conversations, not just a single message. Most of the time, a text message, a voicemail, or even an email is part of a larger conversation. One single text message or email might not be enough to show everything that's happening. Stalking and harassment are usually a series of interactions. When you are capturing the message, try to capture other messages that can help provide background to the threatening or harassing message.

TIP: If you have to scroll up or down to read a text message then you will need to take more than one screenshot. When taking the screenshot, you want to show the court that it's all part of one conversation. Take your first screenshot, and then move the text only halfway so the bottom half of the first screenshot is now the top half of your second screenshot. Repeat this until you capture the entire conversation.

Who Sent the Message?

It's very important to show that whoever sent the message is the person who is abusing or harassing you. You can show this by capturing the person's username, phone number, email address, or any other information that might identify the sender of the message. More information is better because the other person may deny sending the message or ownership of the account.

Remember it may be possible to identify a person by their words, even if the message was sent from an anonymous account. For example, if a person sends you a harassing email with a fake email address, but in the email writes about something that only he or she would know, uses words that she or he regularly uses in other communications, or continues a prior conversation, then that could help show that it is the abusive person, even though the email address is anonymous or different.

When Was It Sent?

If possible, also document the date and time the message was sent. If it was online, this information might show up next to the post or comment. If it was a text message, you might need to tap or swipe on the message to show the date and time it was sent. You might also want to document when you captured the message. Sometimes the date and time is on the phone or computer, and you can include that when you are taking a screenshot. Nearly all devices will allow you to see date and timestamps. If you are unsure, do an online search for “Show date and timestamp on [messaging app] for [your specific phone, tablet or computer].”

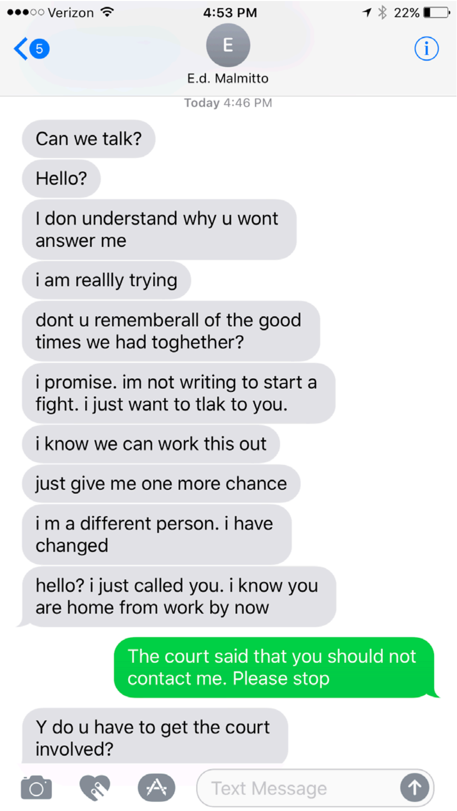
What Should You Capture?

On Your Smartphone

TEXT MESSAGES

- The abusive message, including other text messages that give context to the abusive message.
- The time and date the message was sent. Some message apps can be tricky and hide the time and date. You may need to tap or swipe on the message to show the date and time it was sent. If you aren’t sure how to show the time and date, search online for “show date and time stamp for [your messaging app or phone type].”
- Who sent the message. Include the name and the phone number of the person who sent you the message. If this isn’t apparent from the screenshot you took of the message, go to your contacts and capture a screenshot of the name and phone number of the person who sent you the message. This will show that the message was from that person’s phone number. Make sure that the name

or telephone number is visible on at least one of the screenshot images.



Today 4:46 PM

Can we talk?

Hello?

I don understand why u wont answer me

i am reallly trying

dont u rememberall of the good times we had toghether?

i promise. im not writing to start a fight. i just want to tlak to you.

i know we can work this out

just give me one more chance

i m a different person. i have changed

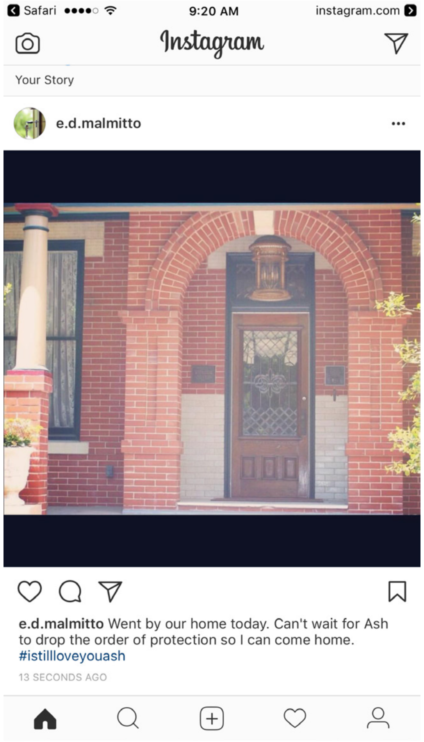
hello? i just called you. i know you are home from work by now

The court said that you should not contact me. Please stop

Y do u have to get the court involved?

INSTAGRAM

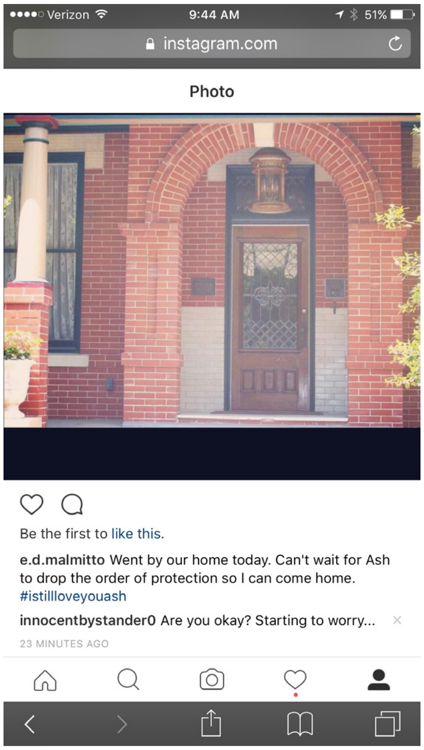
- If it is the Instagram image that is harassing, capture the picture and who posted it. The name of whoever posted the picture will show up above the picture.



e.d.malmitto Went by our home today. Can't wait for Ash to drop the order of protection so I can come home. #istillloveyouash

13 SECONDS AGO

- The comments. If the abuse or harassment was in the comment section, take a picture or video of the username, the image, and the comment. At the bottom of the comment, it will show when the person made the comment. Document the date that you took the image or video.



●●●●○ Verizon 9:44 AM 51%

instagram.com

Photo

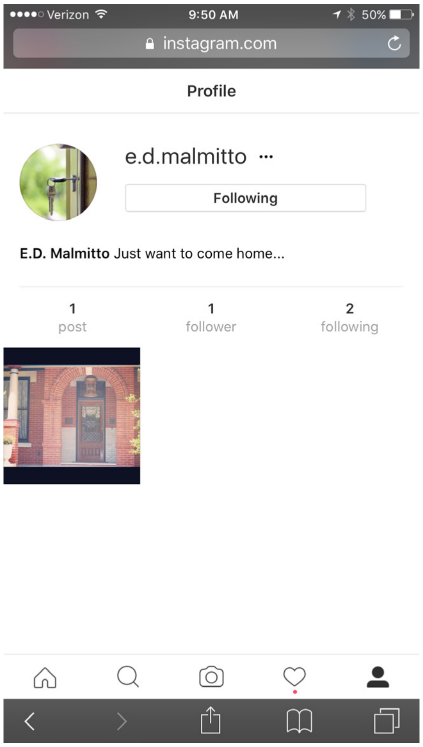
Be the first to like this.

e.d.malmitto Went by our home today. Can't wait for Ash to drop the order of protection so I can come home. #istillloveyouash

innocentbystander0 Are you okay? Starting to worry...

23 MINUTES AGO

- The profile of the person who is harassing you. Tap on the picture of the person to bring up the profile. The profile screen will show the name on the account in addition to a larger image of the profile photo.



●●●●○ Verizon 9:50 AM 50%

instagram.com

Profile

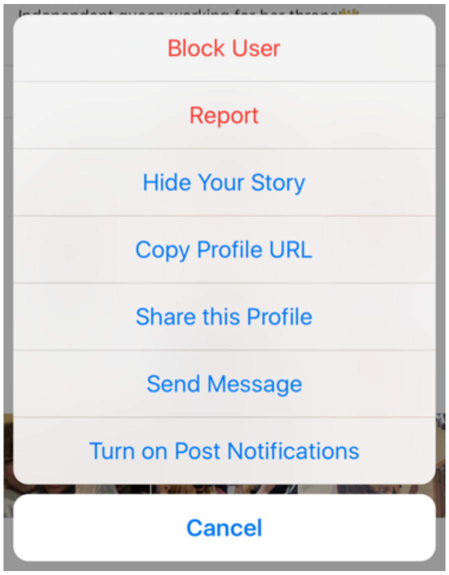
e.d.malmitto ···

Following

E.D. Malmitto Just want to come home...

1 post 1 follower 2 following

- The person's profile URL. When in the person's profile page, click on the 3 dots next to the user name. You can copy the profile URL. You will need to paste it into a document or an email.



SNAPCHAT

IMPORTANT NOTE ABOUT SNAPCHAT:
In recent years, companies have created technologies that automatically delete information, such as text, pictures, and videos, after the information is viewed. Snapchat is the most popular app that uses this technology. This technology can help individuals to increase privacy by limiting the time that another person can access a sender's information. While Snapchat and other similar technology may have some privacy benefits, the technology can also make it very difficult to gather evidence. The whole purpose of sending a "Snap" is for Snapchat to automatically delete the information soon after it is viewed. This function is set up so that even if a professional forensic examiner were to search, a deleted Snap is almost impossible to find. Therefore, if you are being harassed through Snapchat (or another similar technology), you must plan how you will attempt to gather evidence, which includes your own Snaps and Snaps sent by an abusive person. Here are some suggestions for evidence gathering on "disappearing" messages:

- Your own Snaps and Chats. You can choose to save your own posts to Memories or your own Camera Roll, but you can't save other people's posts this way. Saving your own Snaps will keep another person from misstating what you have sent, so it's a good idea. Of course, this could be a dangerous option if the other person has access to your device.

- Other people's Snaps and Chats. After you open a Snap or Chat, you can take a screenshot, but the sender will be notified of the screenshot. You also can choose to save a Chat, but again, the sender is notified. This may not be safe. You should consider your own situation and whether alerting the other person that you've saved the information could be dangerous for you.

- Screen recording apps are built into many smartphones, and you can download other recording apps (some free, some for a small price). Please be aware that some apps may alert the sender of the recording just like a screenshot. (This is true for the iPhone built-in app, but we haven't tested others.) Please make sure it's safe before deciding to record. On the other hand, if you are concerned about someone else recording your Snaps, please know that Snapchat may not recognize all apps and so may not notify you if someone else records your Snaps.

- One way to avoid the notification problem of taking screenshots or using a recording app is to use a second device or camera to take pictures or record. (Again, be aware that this method can also be used against you if you are concerned about your Snaps being recorded by someone else.) Also, this requires having a second device or camera ready and able to record as you review the Snaps sent to you, so you have to plan ahead.

- Don't forget to tell the whole story—if you need to show both the sender's Snaps and your own for context, be sure to organize the screenshots or recordings before presenting them in court. If you do a recording, follow the steps above in the section about video recordings to be sure the court can view your evidence.

On the Internet

EMAIL

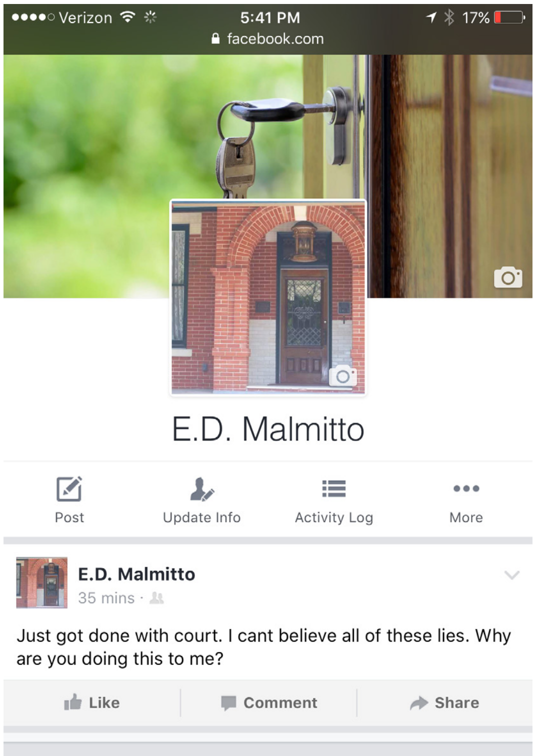
- The email message. You can print out the email, which will show the To, From, Date, and Subject information. A printed email will also show the file name of any attachments. When printing an email, it can change how the email looks and that can make it harder to get the email admitted into court. If the email changes when you print it, you might want to take a screenshot and then print the screenshot instead.
- The header. What you see in an email is often not all of the information available in that email. A lot of information is hidden in what is called the "header." Specifically, the header has information about the IP address (an individualized code that can help to show who sent an email). When printing emails for court, make sure to print the email with the email header. You can find a lot of information online on how to print emails with headers: Just do an online search for "how to print email header in [name of email provider (e.g. Outlook, Gmail, etc.)].
- The IP address. One you have the printed email header, look for the "From" IP address. It will be a long code. You can take that code and enter it into an IP address search (do an online search for IP address search). Generally, you will see a map that shows where an email was sent from. This will not work with all emails, but it will work for many emails.
- If you are receiving email from someone using a fake email address, what is written in the email can help indicate who sent it. If you have multiple emails from one fake email address, you can print all of them to help show that the different emails are from one person.
- If you want law enforcement to investigate your emails, it's important that you don't delete or forward the emails; keep the originals in the email account.

FACEBOOK

To capture evidence from Facebook, here's what you'll need:

- The harassing message or comment, including the name and profile photo of whoever posted the message.

- Profile information of whoever posted the message or the comment. Click on the person's name to be taken to his or her profile page, which should include name, profile picture, and other public information. Even if the other person has made their account private, Facebook will always make publically available the name, username, profile photo, cover photo, gender, and networks.
- If they "liked" or "reacted" to your post, you can click on those who liked/reacted to your post to see a list of those people. Take a screenshot to show that someone interacted with your Facebook post, even if they did not comment.

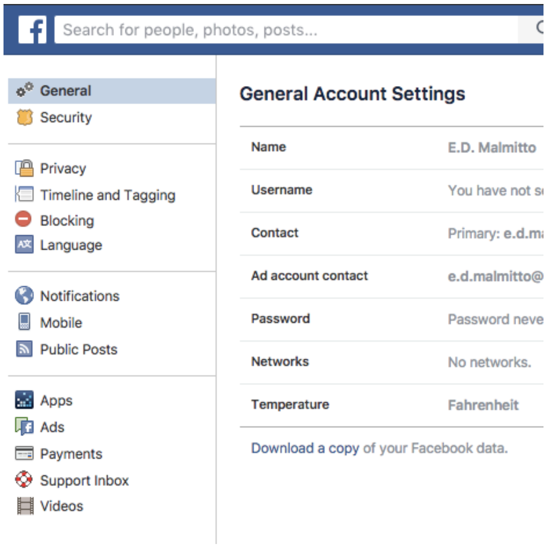


E.D. Malmitto

E.D. Malmitto
35 mins ·

Just got done with court. I cant believe all of these lies. Why are you doing this to me?

- Facebook has the Download Your Information Tool (https://www.facebook.com/help/131112897028467/). This tool will download everything you have ever uploaded or posted on Facebook. Because this option will give you everything you've ever done on Facebook, it can be very long and you may have to go through it to find the useful evidence.



General Account Settings

Name	E.D. Malmitto
Username	You have not s
Contact	Primary: e.d.ma
Ad account contact	e.d.malmitto@
Password	Password neve
Networks	No networks.
Temperature	Fahrenheit

Download a copy of your Facebook data.

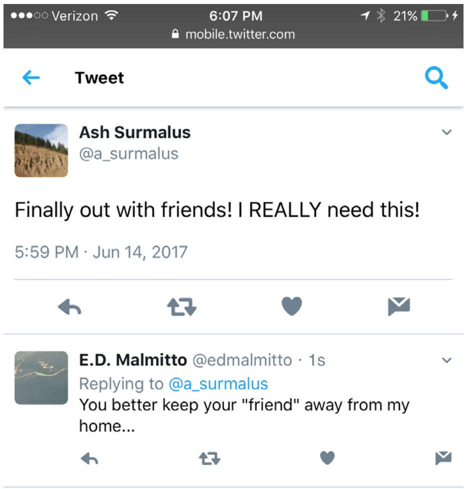
To download your information on Facebook:

1. Sign into your Facebook account.
2. Go to your General Account Settings.
3. At the bottom of the screen, there is a link that says: "Download a copy of your Facebook data."

TWITTER

For Twitter, here's what you need to document:

- The harassing tweet. Harassment on twitter could be more than just one tweet. You may have to take multiple screenshots.



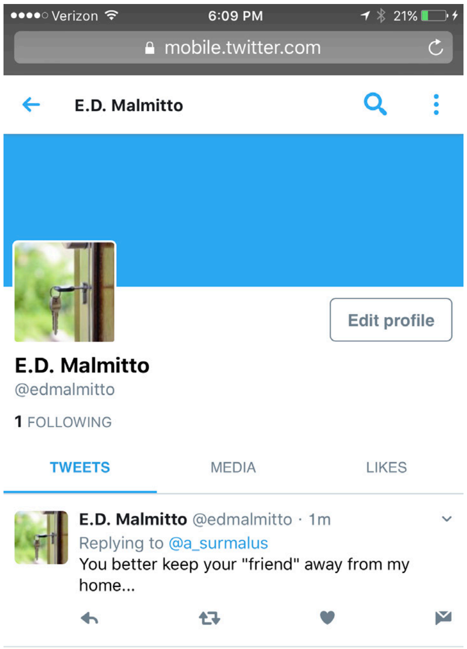
Ash Surmalus
@a_surmalus

Finally out with friends! I REALLY need this!

5:59 PM · Jun 14, 2017

E.D. Malmitto @edmalmitto · 1s
Replying to @a_surmalus
You better keep your "friend" away from my home...

- Capture profile information. Just like other social media, tapping on the photo or name of the person who posted will give you the profile page with additional identifying information.



E.D. Malmitto
@edmalmitto
1 FOLLOWING

E.D. Malmitto @edmalmitto · 1m
Replying to @a_surmalus
You better keep your "friend" away from my home...

- Report abusive message. When you report an abusive tweet to Twitter, you have the option to ask Twitter to email you a report. This report includes: the threatening tweet, the username of the person who tweeted, date and time of the tweet, your account information, and the date and time of your report. This report can be very helpful since it includes all the information you need.

VOICEMAILS

To document an abusive or harassing voicemail, you can write down exactly what was said, but that won't include things like tone of voice. To present the voicemail recording, you'll need the following information:

- The voicemail message, in a format the court can accept (call the court if you're not sure).
- Additional information about the call. Some voicemail services will tell you the number of the person who left you a message and the date and time of the voicemail.
- Phone logs or call history. Your phone logs or call history, which you can find on your phone or on your phone bill, could provide additional information if you can match up the message with the phone number, date, and time of the call on your phone logs. Take screenshots of the phone log. You may have to ask your telephone carrier to give you records, which can take time so plan ahead. If you think you will need records, contact your telephone carrier immediately to ask that they retain your records.
- Note that if you have a digital answering machine (one that plugs into an electric outlet), unplugging it could erase all your messages. It is helpful to make an audio recording of the voicemail messages you want to keep onto a separate recording device in case the original gets accidentally erased and to help to provide the information to the court. You will probably need to record the voicemail onto a DVD or a CD in order to present it to the court.

Next Steps

After you have captured the harassing message by taking a screenshot, a picture, a recording, or a video, your next step may be to use this message in court as evidence. For a step-by-step guide about how to present evidence in court, please read *10 Steps for Presenting Evidence in Court* (https://www.rcdvcpc.org/resources/resource/10-steps-for-presenting-evidence-in-court.html). If you do not have an attorney, you will still need to gather and present your evidence in the proper way as required by the court and your state's law. Courts have "rules of evidence" to help judges make decisions based on good information, not gossip and guesswork. Although the rules can be confusing, they are designed to protect your rights, and you can use them to help you plan for your court appearance. Even though courts work differently, this publication will introduce you to the nuts and bolts of presenting evidence to a court.

You can also read our publication *10 Ways to Find Help With Your Case* (https://www.rcdvcpc.org/resources/resource/10-ways-to-find-help-with-your-case.html), to learn more about finding an attorney or other help with your case.

We wish the best for you and your children.

Additional Resources

For more information about documenting and technology safety:

Documentation Tips for Survivors of Technology Abuse & Stalking (https://www.techsafety.org/documentationtips)

Sample Documentation Log (http://bit.ly/2EC5Dgv)

How to Take a Screenshot (Video) (http://techsafety.org/resources-survivor/screenshot-videos)

Facebook Guide on Privacy & Safety (http://techsafety.org/resources-survivor/facebook)

Twitter Guide on Privacy & Safety (http://techsafety.org/safety-privacy-on-twitter-a-guide-for-victims-of-harassment-and-abuse)

General Technology Safety Information (http://techsafety.org/resources-survivors)

Technology Safety App (http://techsafetyapp.org/)

This document was supported by Grant Number 90EV0439-01-00 from the Administration of Children, Family and Youth Services, U.S. Department of Health and Human Services (DHHS). Its contents are the responsibility of the author(s) and do not necessarily represent the official view of DHHS.

NCJFCJ
est. 1937
NATIONAL COUNCIL OF
JUVENILE AND FAMILY COURT JUDGES
WWW.NCJFCJ.ORG

CELEBRATING 80 YEARS 1937-2017

RCDV:CPC
Resource Center on Domestic Violence:
Child Protection and Custody

FYSB Family & Youth Services Bureau
Family Violence Prevention
& Services Program

Approaches to Evidence Collection: Criminal vs. Civil Cases

The collection and availability of evidence may look different in criminal versus civil cases. This document provides general tips for each system. For more detailed suggestions on investigating evidence from specific types of technologies, see our Evidence Collection Guides.

Criminal Investigations

Generally speaking, criminal cases have a larger selection of evidence available. Criminal investigators often have the benefit of being able to access evidence from both the survivor *and* the alleged perpetrator. For example, many criminal investigations include a forensic professional who can examine the devices for all relevant parties. Additionally, criminal investigators can often access important records from technology companies that are difficult to obtain in civil cases.

Although beneficial, the larger availability of evidence in criminal investigations increases the possibility that the disclosure of sensitive information may cause survivors and other witnesses embarrassment, fear, or misunderstanding. This may impact their willingness to provide access to records, and/or data, unless safety protocols are put in place. It is essential that survivors are informed about what information is being sought out, why it is needed, and how it will be used.

One option is to perform a more focused investigation, by collecting only the data from the survivor’s device(s) that is relevant to the investigation. By NOT doing an entire “dump” of the data, one is able to respect the privacy of the survivor, collect the necessary evidence to further the investigation, and still allow prosecution to fully comply with the *Brady* requirements of providing defense counsel with exculpatory evidence. This more focused investigation may also provide an elevated level of comfort to the survivor and increase their willingness to assist with the investigation.

Civil Investigations

Many civil investigations do not include a forensic professional, and even when forensics are a part of the case, the investigation is generally limited to the client's devices. Similarly, many companies are unwilling to respond to civil subpoenas, even when properly signed by a civil court judge. While some companies may respond to requests for documentation about a person's own account, few will respond to requests regarding the abusive person's account. Because of these limitations, civil attorneys need to be creative to locate relevant information. Civil attorneys will have to rely on evidence the survivor and the abusive person may have access to, and take proactive steps to protect and document evidence.

There is one essential way in which civil investigations have a major advantage. Generally, civil attorneys have many more opportunities to speak with survivors and to get to know their stories. Civil attorneys have attorney-client privilege and other protective factors that can lead to survivors to share more sensitive information. The depth of the relationship can help uncover essential evidence that may be useful for both civil and criminal cases.

Working Together

The needs of survivors of domestic violence, sexual assault, and stalking may vary substantially. Some cases require a civil intervention, while others need the criminal justice system. Some cases need all systems to work together. When investigating the misuse of technology, both criminal and civil investigations have strengths that can be used to increase survivor safety and offender accountability. The strengths of both systems can be leveraged in important ways to the benefit of survivors and the community.

This document is a part of a series that details how to collect evidence related to the misuse of technology in domestic violence, sexual assault, and stalking cases. We recommend that you also read A Primer for Using the Legal Systems Toolkit: Understanding & Investigating Tech Misuse and Approaches to Evidence Collection: Survivor Considerations. The series is part of a Legal Systems Toolkit that includes various detailed guides meant to assist prosecutors, law enforcement, and civil attorneys.

If you have further questions about investigating tech abuse cases, please contact Safety Net, and visit TechSafety.org for more information.

Special thank you to Bryan Franke of 2CSolutions for providing expertise and guidance on the creation of this series.

Supported by US DOJ-OVW Grant No. 2016-TA-AX-K069. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of DOJ. We update our materials frequently. Please visit TechSafety.org for the latest version of this and other materials.

NNEDV

Evidence Collection Series: Emails

Where to begin?

This technology-specific guide is a part of a series that details how to collect evidence related to the misuse of technology in domestic violence, sexual assault, and stalking cases. Before proceeding, we recommend that you read A Primer for Using the Legal Systems Toolkit: Understanding & Investigating Tech Misuse, Approaches to Evidence Collection: Survivor Considerations, and Approaches to Evidence Collection: Criminal vs. Civil Systems.

Who should use this resource?

The series is part of a Legal Systems Toolkit that includes guides to assist prosecutors, law enforcement, and civil attorneys.

IMPORTANT TIP/NOTICE FOR ADVOCATES: If you are a non-attorney survivor advocate, we strongly recommend that you do NOT gather or store evidence for survivors. You can greatly assist survivors by giving them information to gather the evidence themselves. Your participation in the process of gathering or storing evidence can lead to you being forced to testify in court, which can undermine confidentiality protections and negatively impact both the survivor and the integrity of your program. If you have questions, please contact Safety Net.

Email as Evidence: An Introduction

Email messages, whether sent by computer or a mobile device, are a common form of communication. In domestic violence cases, courts routinely order email as a means of “safe” communication between parties, as it leaves a written record. Abusive people frequently misuse email by sending harassing messages, gaining unauthorized access or creating fake addresses in order to monitor or impersonate survivors, or sending computer viruses or spyware. Email evidence can strengthen cases by providing proof of abuse and a clearer picture of relationship dynamics.

Email: The Technology

Despite being common technology, most people do not understand how email works “behind the scenes”. A basic understanding can help when investigating and documenting abusive behavior. In order to ensure clarity, we need to first identify specific terms that will be used in this document.

Email “Client”: An Email client refers to the program used to interact with your email; like Outlook, Gmail, and Yahoo!.

Email Header: This is a log file of sorts, which documents useful information regarding the sending of an email. It also contains information that is specific to that individual email communication. Specific steps need to be taken to view the email header, as it is commonly hidden from normal viewing.

Email Body: This is the content of the email; the message being sent.

Email Signature: An email signature may or may not be present as it is controlled by the user/author. It is typically at the end of the email body. Think of it as the author’s signature at the end of the message.

Email Attachments: An attachment is a file sent with an email and can be an image (picture), a video, an audio file, a document, etc.

Email Evidence: The Digital Trail

While email evidence can be extremely useful, it is not always properly sought out or collected, and it can get accidentally deleted or tainted. The remainder of this document covers how to collect and maintain email evidence to increase its usefulness in court. You can also read more about the differences in technology evidence collection between criminal and civil cases.

Admitting email evidence generally requires showing that an email is relevant to the case and a specific person authored and/or sent it. There are a variety of different ways to accomplish this, including: through agreement, through company records, and possibly through the email itself.

IMPORTANT NOTE ABOUT AGREEMENTS: Frequently, parties will consent to email evidence being admitted into court. It can be useful to consider communicating with the other party (if possible) about whether an agreement can be reached regarding introducing certain messages. It is far easier to introduce the evidence by agreement than to seek out a legal process or fight about the issue in trial.

ABOUT EMAIL AND PRIVACY: Prosecutors and law enforcement, in particular, will want to limit the amount of email evidence that is collected to protect against turning over to defense counsel unnecessary information due to *Brady* requirements. Turning over a victim’s private email information that is not directly relevant to the case can impact the willingness of victims to testify, confuse the factfinder(s), and can lead to unnecessary re-traumatization.

The Body

The body of the email can have important information, beyond what is clearly spelled out in the communication. In cases where the sender of the email is contested, the body may include distinctive vocabulary, information, writing patterns, misspellings or other contextual clues that may help to prove who wrote the email. Additionally, the content of one email in a thread of messages may give important context to the overall communication, or could be used to show that an individual is inappropriately presenting only a portion of a conversation in order to mislead a factfinder.

Signatures

There may be useful information worthy of investigation in the signature(s) in an email or email thread. Signatures are often automatically placed at the bottom of emails, and may even be forgotten about after the initial set-up. Signatures might be included only with new email messages or may look different if the message is a reply or a forward. Some signature may have be legally binding such as the case of "electronic signatures."

Attachments

Evidence contained in email attachments is not always fully utilized. Attachments may have important metadata, or information about the message or the attachment itself, that can help to identify the author/sender.

While it's useful to examine available metadata, make sure that any investigation complies with appropriate ethical requirements. Many states have ethical opinions that preclude using metadata that was accidentally sent. This is particularly true where one attorney has inadvertently sent metadata in a document that provides protected information about another client. It is important to be aware of your jurisdiction's ethical rules on this issue.

The Header

The header of an email carries important metadata including the sender, receiver, date, time, subject, and Internet Protocol (IP) address. The IP address of the sender may allow investigators to determine where the email was sent from and possibly who sent it. Note that an IP address may be challenging to connect with a sender if an anonymous proxy server or a relay service was used.

It is important to note that accurate header information is only available in the original[1] electronic version of the email. That version may be accessed through a computer or mobile device, through a web mail platform or account, or on an email server itself. An investigator will not be able to view the original email header by having the survivor forward the email to them. In a forward, the original email header is replaced with a header that contains the forwarder's

[1] "Original" is a complicated term because digital files "live" in so many places simultaneously. In this case, original primarily refers to a message that has not been "forwarded" or sent as a part of a "reply."

information. It is also not possible to uncover the header with just a screenshot or photo of the email body. It is also possible for the survivor to copy/paste the email header into a new document and send that or a screenshot of the header to the investigator as an attachment to an email. The survivor may also log into their email from a computer at the investigators office and retrieve the email header while the investigator watches to ensure the integrity of the data. Law Enforcement investigators should validate this information by serving legal process on the email company to obtain not only the email communication(s) in question, but the associated email header(s) as well. Legal process should also be served on the suspect's email account that was used to send the email(s) in question, requesting copies of all sent mail, draft mail, and access logs during the same time frame of the evidentiary emails. This will help provide a more complete picture of events and help rule out someone else accessing the suspect's email account and sending the email(s) in question.

While it is important to maintain the integrity of the original email message, remember that multiple copies may exist in backups of servers or devices, even if the survivor thinks that the original was deleted.

What is an IP address?

IP addresses have been successfully used to identify abusive persons. It is helpful for the survivor to keep a log of abusive behaviors and to document IP addresses from those electronic communications.

An IP address will appear in one of two ways; as a numerical code or a combination of numbers and letters (hexadecimal digits). It is used to identify a particular device on the Internet. Every device requires an IP address to connect to the Internet. There are two versions of IP addresses; IPv4 (version 4) and IPv6 (version 6). IPv4 consists of four sets of numbers, each ranging from 0 to 255, and each set separated by a dot, for example "66.72.98.236" or "216.239.115.148". IPv6 consists of eight groups of four hexadecimal digits, each separated by a colon, for example "2001:4860:4860:0000:0000:0000:0000:8888". With IPv6, the IP address is often displayed in a truncated format. That is done by removing the sets of four hexadecimal digits whose value are all “0” and replacing them with an additional colon, for example “2001:4860:4860::8888”.

There are two types of IP addresses that can be assigned by an Internet Service Provider (ISP). A **static IP address** is always the same, while a **dynamic IP address** may change every time a user connects to the Internet. A dynamic IP address is most common for home users. An ISP, will have records of which customer was assigned a particular IP address at a specific date and time. This is how a residence/location can be associated with a particular IP address. ISP’s typically keep these records for no more than 90 days.

Finding the IP Address

The header in an email will often contain the IP address that the email was sent from. To find the originating IP address, that is the IP address used to send the email, read the email header from the bottom up and look for the IP address that follows the “x-originating-ip” or “Client IP”. In some cases, the “x-originating-ip” or “Client IP” address shown in the email header may not be the one issued to the sender of the email by the ISP. If you lookup the IP and find Google or an email provider, they may have substituted their IP for the originating (sender’s) IP. In this case, they will likely still have the sender’s IP address on file and can provide it if served with appropriate legal process.

Locating an email header varies depending on the email client. To find instructions for locating headers, try an online search for “How to see full email headers in [name of email client].”

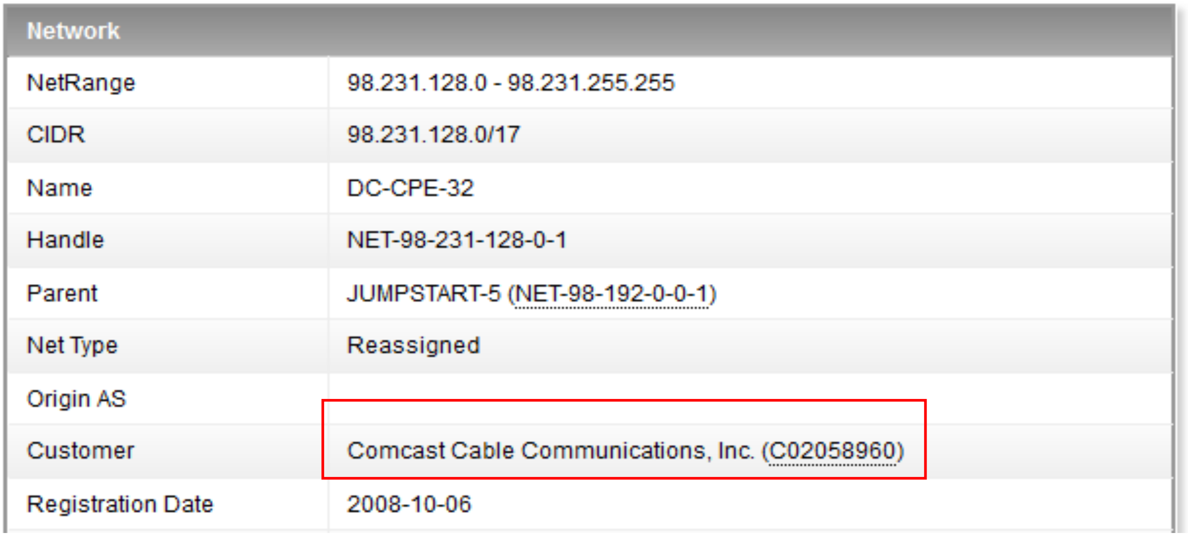
Looking up or Tracing an IP Address

Once you have the x-originating-IP or Client IP address, you can find the ISP that is leasing the IP Address by performing a “WhoIs” search. There are several different online resources to locate this information, a commonly used one is www.arin.net. Some of these sites will also provide other information, including the approximate geographic location of the device assigned to that IP address.

This location information may not be reliable or accurate enough to be used for anything more than a general city within a state.

The following is an example of a complete email header, noting in red the X-Originating-IP and the Message ID, a unique ID given by the originating SMTP email server that can help identify the sender, even if the “From” was tampered with.

```
Return-Path: <bo-bwzv75gbruqgjvau79gjgqcd1etmfu@b.e.redbox.com>
Received-SPF: pass (domain of b.e.redbox.com designates 8.7.43.55 as permitted sender)
 d2luZyBvbiBhIG1vYmlsZSBkZXZpY2U_IENsaWNrIGhlcmU8L2ZvbnQ.PC9h
 →X-Originating-IP: [8.7.43.55] - (Originating Address)
Authentication-Results: mta1468.mail.mud.yahoo.com  from=e.Redbox.com; domainkeys=pass
(ok);  from=e.Redbox.com; dkim=pass (ok)
Received: from 127.0.0.1  (EHLO mta935.e.redbox.com) (8.7.43.55)
  by mta1468.mail.mud.yahoo.com with SMTP; Mon, 09 Jan 2012 23:21:10 -0800
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; d=e.Redbox.com;
            s=20111006; t=1326180070; x=1341904870;
            bh=vHcWxB+fko8JnzSoHgJq7o0Sb60=; h=From:Reply-To;
            b=aq2hXhNIClf/rE/ckB6HCT+mq94XLXa0gooqa1fP8ZDfLlo0RQ1H8WkbwK/
 h=Date:Message-ID:List-Unsubscribe:From:To:Subject:MIME-Version:Reply-To:Content-type;
Date: Tue, 10 Jan 2012 07:21:10 -0000
→Message-ID:
<bwzv75gbruqgjvau79gjgqcd1etmfu.14711394101.8250@mta935.e.redbox.com> (Message
ID)
List-Unsubscribe: <mailto:rm-0bwzv75gbruqgjvau79gjgqcd1etmfu@e.redbox.com>
→From: "Redbox" <Redbox@e.Redbox.com> (Sender’s email address)
To: 1234567@yahoo.com
Subject: This week's new releases
MIME-Version: 1.0
Reply-To: "Redbox" <support-bwzv75gbruqgjvau79gjgqcd1etmfu@e.redbox.com>
Content-type: multipart/alternative; boundary="=bwzv75gbruqgjvau79gjgqcd1etmfu"
Content-Length: 66578
```

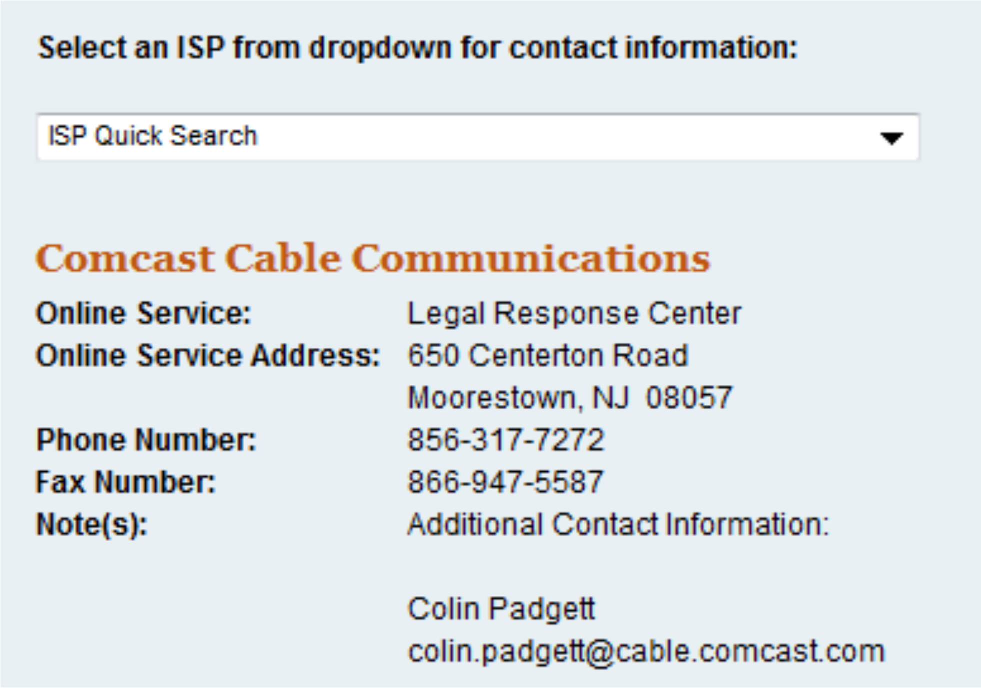


Network	
NetRange	98.231.128.0 - 98.231.255.255
CIDR	98.231.128.0/17
Name	DC-CPE-32
Handle	NET-98-231-128-0-1
Parent	JUMPSTART-5 (NET-98-192-0-0-1)
Net Type	Reassigned
Origin AS	
Customer	Comcast Cable Communications, Inc. (C02058960)
Registration Date	2008-10-06

Contacting the Internet Service Provider (ISP)

The ISP can identify who the IP address was assigned to. In some cases, it may be an individual home, linking directly to the abusive person, or it may be to a hotel, library, coffee shop, or other location, in which case you would need to establish that the abusive person was there through other evidence, like security surveillance footage and connection logs for the public WiFi that was used.

Most ISP's will have a specific contact for law enforcement. You can search for that specific contact information on the ISP List at Search.org, for example:



Select an ISP from dropdown for contact information:

Comcast Cable Communications

Online Service: Legal Response Center
Online Service Address: 650 Centerton Road
Moorestown, NJ 08057
Phone Number: 856-317-7272
Fax Number: 866-947-5587
Note(s): Additional Contact Information:

Colin Padgett
colin.padgett@cable.comcast.com

With a Retention Notice or Preservation Order, the ISP will create a copy of the data identified in the order and maintain that information until served with the appropriate legal process, or 90 days passes. A Preservation Order is generally only valid for 90 days; however, one additional Preservation Order may be provided to the ISP, thereby adding an additional 90 days to the length of time for a total of 180 days. This is a critical step to ensure information is still available until a subpoena, court order for production of records, or search warrant can be obtained. A subpoena or court order for production of records can allow you to obtain basic subscriber information, whereas a search warrant can get access to actual email content.

Be aware that the ISP may attempt to notify the abusive person that legal process has been served on them regarding their account. To decrease safety risks to the victim, include in the subpoena, court order for production of records, or search warrant specific orders to the ISP not to notify the account holder/customer (the abusive person) or make any changes, like locking access to the account. Some ISP's require a separate/stand-alone court order mandating they not disclose the service of legal process to the account holder/customer (the abusive person).

Some ISP's may state that they will charge a fee for the processing of the requested information. Informing them that the fee is not feasible often results in it being waived. In some jurisdictions, it may be possible to ask the court to make the offender pay for the cost of processing requests to the ISP.

Connect an IP Address to a Specific Person

This last step can be the hardest part of an investigation. In some cases, locating the IP address and putting that information into an IP lookup can give you helpful clues about the geographic coordinates of the sender. Unfortunately, that evidence may not always be admissible or available. In many cases it will be necessary to build circumstantial evidence to show that the IP address is connected to a device owned or used by the alleged perpetrator and that the perpetrator had access, motive, and opportunity to use the device.

Tips for Collecting Email Evidence

TIP 1: Consider Emails Received and Sent

It is important to talk with survivors about email communications with the abusive person and *also* about any suspicious or malicious communications that may have come from the abusive person through impersonation. Sometimes survivors may not discuss things that they feel like they cannot prove. For example, survivors may be reluctant to discuss or report that a person had inappropriately used their email address to send messages, while pretending to be the survivor, because they are embarrassed about the messages or because they may fear that they cannot prove that it was the abusive party. Let the survivor know that it is your job to help prove who sent it, their job is to let you know everything that has happened, including things that may be embarrassing or difficult to prove.

TIP 2: Protect Against Inappropriate Access

There are a variety of ways that an abusive person could falsify email evidence. They could unlawfully access a survivor's email account to delete or send inappropriate emails. They could also set up a fake account that has an address similar to the real account (e.g. terry.smith@company.com might be faked as terrysmith.company@gmail.com), or might use an email spoofing service. Or they may use impersonation to try and paint survivors in a negative light. It is important to be aware of these possibilities and to be prepared to help the court understand them.

Many email clients allow for the account holder to see what devices accessed an account. Some even provide information about the date, time, Internet browser used, and approximate geolocation for each device. It is important to help survivors set up strong passwords and to ensure that the survivor has a system to regularly check which devices are able to access their accounts.

Next Steps in your Investigation

Despite the challenge that technology can pose to evidence collection, it *is* possible to successfully prove tech abuse cases through effective investigation and creative advocacy. Help the survivor understand how to protect, collect, and preserve evidence. Read more about the importance of involving survivors in the process of collecting evidence in Approaches to Evidence Collection: Survivor Considerations. Survivors' active participation can lead to information that may strengthen the case, and can give survivors essential tools for safety and healing regardless of the outcome of the case.

For more information, see the resources in our Evidence Collection Series. If you have further questions about investigating tech abuse cases, please contact Safety Net, and visit TechSafety.org for more information.

Special thank you to Bryan Franke of 2CSolutions for providing expertise and guidance on the creation of this series.

Supported by US DOJ-OVW Grant No. 2016-TA-AX-K069. Opinions, findings, and

conclusions or recommendations expressed are the authors and do not necessarily represent the views of DOJ. We update our materials frequently. Please visit TechSafety.org for the latest version of this and other materials.

NNEDV

Evidence Tips for Prosecutors:
Technology Abuse

In today’s digital age, prosecutors need to know how to prosecute cases that include technology-related evidence. This resource will give tips on how to more effectively prepare a case that involves the misuse of technology.

Technology can provide evidence where it might not have existed before; capturing important communications and offender actions. Though technology may initially appear intimidating, the rules of evidence are generally sufficient to include evidence from new technologies. For example, the process to admit a handwritten note is fundamentally the same method used to admit text messages from a digital device. In many cases, admitting tech evidence is very similar to the process of admitting more traditional forms of physical evidence.

Please note that this tip sheet is not intended to be legal advice.

This document is a part of a series that provides tips and considerations for collecting evidence related to the misuse of technology in cases involving domestic and sexual violence or stalking. Other topics in the series include collecting evidence related to emails*,* telephone calls*,* social media, online images and videos, spyware, electronic surveillance, and location tracking.

Before proceeding, please make sure to read the Primer for Using the Legal Systems Toolkit. It contains information that is essential to understanding all of the documents within this toolkit.

Who should use this resource?

This resource was created specifically for use by law enforcement and prosecutors. While survivors and other allied professionals may find the information useful, it’s important to know that the recommendations are specifically geared toward those working within legal systems.

IMPORTANT TIP FOR ADVOCATES: If you are a non-attorney victim advocate, it is strongly recommended that you do NOT collect or store evidence for clients. While helping clients to gather evidence can be of great assistance, it is important that you give the survivor the skills to gather the evidence rather than gathering it or storing it yourself. Gathering or storing evidence can impact the chain of custody and can lead to you being forced to testify about the collected or stored evidence. Testifying in court can undermine confidentiality protections, and negatively impact both your client and the integrity of your program. If you have questions, please contact Safety Net.

Pretrial Considerations

Empower Survivors

While investigators often have specialized expertise in unearthing evidence, it is important to remember that survivors have a great deal of knowledge about their own experience and can be essential to locating useful evidence. Seek out assistance from the survivor whenever possible, identifying what types of evidence you are looking for and specifically letting them know what you plan to do with the evidence. Make sure to let the survivor know whether they will be able to object to the use of certain evidence that is uncovered and what requirements you may have to turn over evidence, including embarrassing content. Trust is essential to locating evidence and to ensuring victim participation.

Build an Evidentiary List

Organization is essential to presenting a successful and seamless case. Make a list of all the evidence that you plan to introduce (technology and non-technology-related). Next, determine the form in which you intend to enter this evidence and write this next to the evidentiary item. For example, if you are trying to admit text messages, determine whether you will introduce printed screenshots, a forensic analysis of a mobile device by police investigators, testimony by a witness, or some combination of evidence. Make note of whether there is any supporting evidence and what process you will use to try and admit the evidence. At times, the process for the primary and supporting evidence may be the same, for example, a witness or business records may be used for both types of evidence. If a witness will be used, write down the witnesses' name next to each item you will be introducing. Authentication is a critical component of admitting evidence. You should identify how you plan to authenticate each piece of evidence. Here is an example of a table that might be helpful.

Evidence Type	**Form of Evidence**	**Supporting Evidence**	**Process of admitting evidence**
Harassing Text Messages	Screenshots	Certified telephone records	Business records and testimony from [Name or witness] that they saw the messages.
Email Messages	Subpoenaed records from email company	Witness testimony that messages were received.	Testimony from [Name or witness] that messages were received.

Authenticating Evidence

Authentication is the process of proving that a piece of evidence is *more likely than not* what you claim it to be. The federal rule of authenticity can be found in FRE 901.[1] You do not need to prove authenticity beyond a reasonable doubt. However, while the standard for authenticity is low, you still have the burden of proving to a court or jury that the evidence helps to prove your case. To do that, you will need to show that the evidence is what you say it is and that the evidence is attributable to the source that you say created it. When authenticating evidence there are two steps you will need to follow:

[1] State evidence rule may vary, but many states mirror the federal rules. Check your state's rules to ensure compliance with local and state evidence guidelines, including the court rules, which may have specific requirements about how to present evidence.

Step 1: Show that the item is what you claim it to be. This is where the list you made during pretrial prep comes in handy. For instance, if you are seeking to introduce a text message you will have your witness testify that they received the message on X date and at Y time and from a number associated with the offender.

Step 2: *Tie the evidence back to the offender*. A text message is a perfect example of how challenging it can be to tie digital evidence to an offender. To link a text message, you must show that the message was sent from a device that the offender had access to, and also that it was the offender who authored the message. It is not enough to show the message came from the offender's email address or cell phone number. Authentication of messaging evidence requires proof of authorship. Proof that a person had exclusive access to a device during the relevant time period is often sufficient and is regularly proven through circumstantial evidence.

Technology evidence can often be linked to the offender through a digital trail, including an IP (Internet Protocol) address, digital forensics, or business records from technology companies. Frequently, technology evidence is authenticated through testimony, including from a victim or law enforcement. However, proving that an offender authored a message may require circumstantial evidence. For instance, certain words or content used in the message or the way a message is written can help to prove that only the offender would have authored it.

**Note: Each piece of evidence you are admitting will need to be individually authenticated. For example, do not assume that because one text message is authenticated that the rest of the chain is also authenticated.*

Don't Fear Motions in Limine

Opposing attorneys may seek to limit your ability to present evidence by filing a pretrial motion *in limine.*[2] While pretrial motions can be challenging, these

[2] Motions *in limine are usually filed to preclude evidence from trial. In some jurisdictions, the party seeking to introduce evidence may also file a motion* in limine to seek a ruling from the court about the admissibility of their

challenges have the benefit of providing a sense of whether the court is knowledgeable about your type of evidence. If the court is not familiar with the evidence, you have the opportunity to educate the judge prior to trial. Additionally, pretrial motions allow you to present key points of your case and to get a sense of how the court may rule. Lastly, the court's ruling may help you correct any deficiencies or problems in your case. Lastly, getting advanced rulings on your evidence helps to ensure that you do not have to argue about your evidence in front of the jury and that you will not have to unexpectedly proceed without a key piece of evidence.

Anticipate and Prepare for Objections

Even after pretrial motions have been decided, it is important to be prepared for possible objections. Anticipating objections will help you to keep your composure, prepare your response, and keep the jury focused on your case and not the issue opposing counsel is raising. For every piece of evidence, be prepared to argue why an objection should be overruled. Below is a list of common objections, though it is a good idea to familiarize yourself with your jurisdiction's rules in order to protect against uncommon objections as well.

- Hearsay (FRE 801(c))
    - Hearsay Exceptions (FRE 803)
- Relevance (FRE 401)
- Unfair Prejudice (FRE 403)
- Best Evidence Rule (FRE 1001-1002)
    - Best Evidence Rule Exceptions (FRE 1003)
- Lack of authentication (FRE 901)

Prepare the Victim

Confronting the abuser in court can be extremely difficult for a survivor of domestic or sexual violence. Preparing the survivor on what to expect during the course of the trial will go a long way in easing the anxiety and trepidation they may be experiencing. The survivor's testimony is often times the best piece of

own evidence.

evidence. Therefore, preparing this testimony is just as important as preparing all the other parts of your case prior to trial.

When you meet with the survivor you will want to describe what they can expect during the trial itself. Explain what the courtroom will look like, where people will be seated, and what to expect during the proceeding. Make sure that the witness has all of their documentation in order so that if their memory needs to be refreshed while testifying you have that on hand. Depending on the level of trauma experienced it is possible the survivor will not recall precise dates and times, particularly in a chronological order.

Other items you will want to discuss prior to the trial date include where the court house is located, where parking is available, and if cell phones are allowed in the courtroom. It’s easy to forget that people may not know these details. It’s also critical to help survivors to identify any possible threats to their safety. For instance, does the witness need to be escorted to the courtroom? Should the witness park in a different location so the offender does not have access to the car? These are all important considerations when working with survivors. Finally, have these discussions well in advance of the trial date so there is time for the survivor to process the information and for you to make necessary safety arrangements.

Trial

Completing the above processes will help to make your case more successful. However, during all aspects of the trial including the proceeding and recesses, you should pay attention to any behavior by the offender or others which aims to intimidate, threaten, or frighten the survivor. These behaviors may be discreet or only have a meaning that is understood by the survivor. Frequently, offenders will send text messages or have other people call the survivor around the time of the trial. It is important to ask about any inappropriate communication and to report any of this behavior immediately to the judge and opposing counsel.

Sentencing

Be prepared to argue all of the facts, including those not allowed into the trial, in order to receive your requested sentence. This might include any danger or threat assessments that were conducted pre-trial, the defendant's past history including any violations (this will usually be done through a pre-sentence report), or the type of technology misused by the defendant.

Sentencing can be an extremely powerful opportunity for a survivor to speak freely about their experience. The victim impact statement can be persuasive, impactful, and cathartic. Consider what special conditions of supervision you will want for this particular defendant, including if there are any technology-related provisions. At this point in the case, you should be intimately aware of the types of technologies misused by the offender. Argue for special conditions or prohibitions that will address technology misuse. Finally, do not forget to argue for any restitution owed to the victim. There is usually a monetary cap for the amount that can be ordered by the court and so also consider referring the survivor to other sources of relief such as the Crime Victims Fund.

Supported by US DOJ-OVW Grant #2016-TA-AX-K069. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of DOJ.

We update our materials frequently. Please visit TechSafety.org for the latest version of this and other materials.

Evidence Collection Series:
Internet of Things (IoT)

Where to begin?

This technology-specific guide is a part of a series that details how to collect evidence related to the misuse of technology in domestic violence, sexual assault, and stalking cases. Before proceeding, we recommend that you read A Primer for Using the Legal Systems Toolkit: Understanding & Investigating Tech Misuse, Approaches to Evidence Collection: Survivor Considerations, and Approaches to Evidence Collection: Criminal vs. Civil Systems.

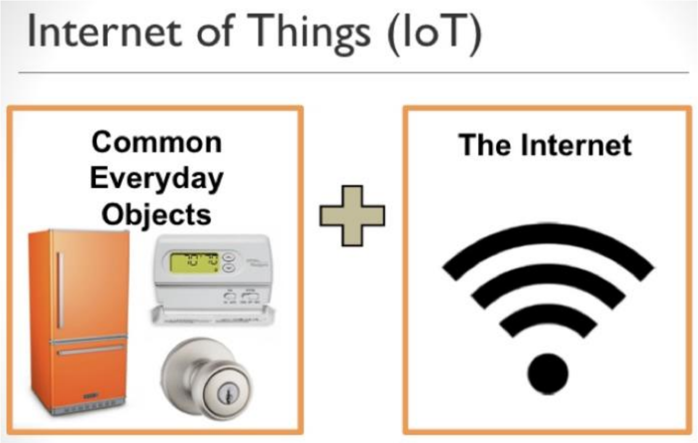
Who should use this resource?

The series is part of a Legal Systems Toolkit that includes guides to assist prosecutors, law enforcement, and civil attorneys.

IMPORTANT TIP/NOTICE FOR ADVOCATES: If you are a non-attorney survivor advocate, we strongly recommend that you do NOT gather or store evidence for survivors. You can greatly assist survivors by giving them information to gather evidence themselves. Your participation in the process of gathering or storing evidence can lead to you being forced to testify in court, which can undermine confidentiality protections and negatively impact both the survivor and the integrity of your program. If you have questions, please contact Safety Net.

IoT: An Introduction

The term or phrase Internet of Things (IoT) refers to a wide variety of devices with different purposes, functions, and capabilities. IoT devices may be connected and controlled through the Internet, Bluetooth, or other means, which makes them practical and efficient tools that can be used to improve quality of life. Survivors can also use IoT to increase their safety. However, these devices or systems can also be misused to monitor, harass, threaten, and isolate. More information about the risks and benefits of IoT devices can be found at TechSafety.org.



IoT devices themselves are not the problem, but rather the misuse of them. For domestic violence, sexual assault, and stalking survivors, the intimate role IoT devices play in people's lives can pose an especially dangerous risk.[1] Investigating IoT abuse can be challenging since the devices can be used to *remotely* harass or threaten victims.

As with most technologies, there are many ways that IoT can be misused. While the possibilities of misuse are evolving with the devices, we will discuss some of the more common types of IoT misuse currently known.

IoT: The Technology

To assist in investigating and uncovering IoT misuse, this section provides examples of different kinds of IoT devices, possible misuses, and security suggestions.

IoT devices are commonly in the home or worn as an accessory, and may be misused to harass or track a victim's movement. The following chart provides examples of common IoT items that can be misused or that may contain useful evidence.

[1] https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html

Smart Appliances: Speakers, home assistants (e.g. Amazon Alexa, Google Home), kitchen appliances, TVs, etc.
Smart Home Systems: Doorbells, thermostats, lighting, security cameras, baby monitors, etc.
Wearable Items: Health trackers (e.g. FitBit), medical devices (e.g. pacemakers), sleep trackers, eye glasses, watches, panic buttons, mood sensors, clothing, etc.

Ways to Connect and Access IoT Devices

- ***Apps and Websites:*** Many IoT devices communicate with other devices, like a smartphone, through the use of apps or websites. These apps or websites enable a user to manage the IoT device settings and to track activity. There are also apps, like Wink Hub[2], that allow users to connect all their IoT devices on a single app for convenience.

- ***Networks:*** A network is what connects different IoT devices and allows them to "speak to each other". This is typically a WiFi network in someone's home. IoT devices can also connect to each other via Bluetooth. For example, a survivor's Alexa home assistant can communicate to their smart speaker system, so that when a song is requested to Alexa it automatically plays on the home speakers.[3] Because many IoT devices share a network, each individual device is only as secure as the most vulnerable device connected to that network. Any insecure device on the network can potentially serve as a doorway into all the other devices. Therefore, it is essential to examine whether the network itself has been breached and whether there are ways to increase the security for all connected devices, and their systems.

- ***Multiple Device Access:*** Most IoT devices are designed to connect to multiple mobile devices (e.g. smartphones) at the same time. It is not uncommon for individuals in intimate relationships to share access to their IoT devices, which

[2] https://www.wink.com/products/wink-hub/

[3] WiFi networks function using the internet while Bluetooth is a separate technology that connects devices that are near one another. https://www.techopedia.com/2/27881/networks/wireless/what-is-the-difference-between-bluetooth-and-wi-fi

means that those devices may have multiple mobile devices that are connected to their network, with or without the knowledge of the survivor.

IoT and the Law

Unlike many other consumer products, there are no federal regulations specifically for IoT products and few if any laws that specifically regulate IoT activity. Some devices, like those used in medical institutions, are regulated because of the laws already covering those industries. The National Institute of Standards and Technology (NIST), has studied IoT devices and created a list of general IoT safety standards, including security risks like hacking and data breaches.[4]

Currently, laws that specifically make abuse through IoT devices a crime are lacking, although many other existing laws may apply. Laws that focus on abusive behavior, such as harassment, spying or surveillance, intercepting communication or eavesdropping, or stalking may be able to be applied in some IoT abuse situations. It may require creatively using available laws. For example, inappropriate access to a victim's IoT device or network without permission, could result in a computer-related crime or a civil lawsuit for invasion of privacy (or similar laws). A victim may also be able to request a protection order if they believe they have experienced abuse and are at risk of IoT abuse. A protection order can include provisions that require the abusive person to not interfere with IoT devices or related accounts, and to remove themselves from those accounts. Proactive protective order provisions may help prevent future incidents.

While the law catches up to the technology, IoT evidence is already making its way into the court system. In a recent case, evidence from a murdered victim's FitBit was used to help prosecute her husband.[5] The increased use of IoT technology is leading to an explosion of new information that may prove indispensable in proving future cases.

[4] https://www.nist.gov/topics/internet-things-iot

[5] https://www.nytimes.com/2017/04/27/nyregion/in-connecticut-murder-case-a-fitbit-is-a-silent-witness.html

Investigating IoT Devices

The first step when investigating IoT abuse is to help survivors identify internet connected devices in their homes, work, transportation, including things they use or wear to determine whether those devices, are being misused, or have been breached. If so, they may contain valuable evidence.

Sometimes it can be difficult to know which devices are Internet-connected. Smart speakers, TVs, or home assistant devices are more commonly understood to connect through WiFi. However, victims don't always know that many common items (like refrigerators, thermostats, and toys) can be connected to the Internet or shared networks. Survivors may have difficulty identifying all of the places to look for Internet-connected devices, systems, and products. It can be helpful to provide a list of common IoT devices, such as the chart on page 3. Knowing which items are at risk can help guide safety planning strategies and evidence collection.

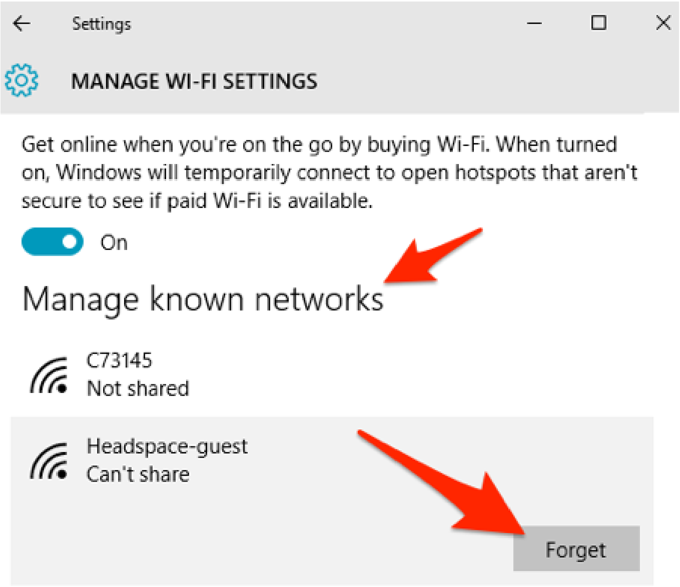
One strategy for identifying what is connected to their network is to access their WiFi router. The router keeps a list of all connected devices, as well as what IP address they have been assigned and other network related information. This will show what is connected, both wirelessly or by a cable, but it will NOT tell you what is connected to another device via Bluetooth.

Tips for Getting Survivors Involved in Evidence Collection

Help the survivor understand how to protect, collect, and preserve evidence. Read more about the importance of involving survivors in the process of collecting evidence in Approaches to Evidence Collection: Survivor Considerations. Survivors' active participation can lead to information that may strengthen the case, and can give survivors essential tools for safety and healing regardless of the outcome of the case.

Look for Shared Devices and Networks

- If the abusive person shares or has shared a home or any device with the survivor, then they could have direct access to those devices or to the accounts that control them. For example, an abusive person who knows the password to a thermostat system could control the thermostat remotely, anywhere the abuser has internet access.
- An abusive person can also misuse an IoT device by downloading spyware or hacking into the actual device, network, or account linked to the device. Certain apps can scan devices to see who is connected to a network or router if the user is near the victim's network, but they do not always work in locating abusive persons operating from a greater distance. An important first step is to identify which devices are connected to the IoT network. Generally, that information is found by locating "settings,"
exact steps may differ depending upon the device and network. An online search for "how to find out what devices are connected to [name of IoT]" will provide further information in most cases.



Get online when you're on the go by buying Wi-Fi. When turned on, Windows will temporarily connect to open hotspots that aren't secure to see if paid Wi-Fi is available.

Document Changes or Suspicious Activity on Account

There may be vital information available in the survivor's apps, websites visited, account information, passwords, and device settings. Sometimes a simple password change, being locked out of an account, or an unusual change in a survivor’s app settings can show that an abusive person has accessed or tried to access the device. However, it is not always easy to identify some of these clues. A more in-depth search of the information or account by a forensic investigator may be required.

Changes in settings or account information should be documented by videos, photos, or screenshots, if possible. Many IoT devices also have online or in-app activity logs, which can be useful in identifying misuse. Some additional options to explore for evidence are:

- A message or notification that a password has been changed without the survivor’s knowledge
- Any change in identifying information (name, address, phone number, etc.)
- Any change in functional settings (e.g. temperature selected, doorbell ring option, any automatic feature by the user)

Track Usage and Timing

Any changes or suspicious activity in the real-time use of the IoT devices should also be documented. Are lights turning on without the survivor initiating it? Are devices making unusual noises? Does the abusive person have knowledge of any incidents involving the survivor or their private information that could have been learned through an IoT device?

Physical observations should be logged and whenever possible, a safe device should be use to take videos, photos, or recordings as proof. A log of strange activity can be important to understanding the full scope of the misuse. The timing of misuse can be compared to the normal activity of the survivor.

Accounts linked to the IoT devices can also provide information about unusual activity. Screenshots or printed copies of this logged information can then be compared to any unusual activity captured live by videos, photos, or audio recordings. Whenever possible, screenshots or videos should include date and time. Proof of digitally logged activity combined with physical evidence of the activity can strengthen a case.

Law Enforcement May Need to Investigate

Law enforcement are usually the first to interact with survivors once a crime has been reported, which means they play a significant role in the early stages of collecting evidence. Law enforcement generally have the tools to do a more advanced search of devices and networks. If the survivor makes an informed decision to involve law enforcement, it may strengthen the ability to search the actual hardware of the devices, as well as their linked accounts and networks. Some examples of evidence that may be more accessible in criminal investigations include (but are not limited to):

1. Records on the abusive party's device that show it was used to remotely control IoT.
2. IoT company records including the IP addresses of remote sign-ons, which can be compared with the abusive person's IP addresses.
3. The abusive person's online activity via WiFi network or ISP, that shows evidence of IoT abuse against the survivor.

Get a Court Order to Collect Records

If the information is not available through the account or the survivor does not have access to the information, a court order for the records might be necessary to collect evidence of IoT activity. Gaining access to account records for IoT apps and websites, WiFi networks, or the abusive person's own devices, networks, smartphones, or computer activity can help prove misuse. At the very least, it can help strengthen a survivor's case.

Differences Between Civil and Criminal Investigation

The process of evidence collection may look different depending on whether the investigation is for a criminal or civil case. While survivors will be important resources in all case types, the evidence available may differ. Approaches to Evidence Collection: Criminal vs. Civil Systems discusses important differences in the two systems and offers tips for professionals in each system.

IoT Safety Tips

If a survivor thinks they are at risk or has already experienced IoT abuse, the following general security tips may be useful.

Create Separate Networks

IoT devices are convenient in part because they rely on shared networks. This same network can then also be linked to a user's email, mobile, and other online accounts. Networks can be private and require a password or they can be public, meaning anyone who is physically close enough to the WiFi can connect and use it. Read more information about WiFi network security.

Create Strong Passwords

Make sure all WiFi network, accounts, and websites linked to the IoT devices have strong passwords. Discuss with survivors the importance of protecting passwords, especially if there is a higher risk of IoT abuse. Read more about strong passwords.

Regularly Update IoT Devices

Software updates include security improvements. IoT users should regularly check for available updates, so their devices have increased protection against hacking or spyware. Updating devices does not eliminate all risk, but it can significantly strengthen device and network security.

Hit Mute and Block Camera

With IoT devices that record audio or images, it is generally a good idea to block the lens of cameras when not in use and to mute sound recording options. If they are hacked into or accessed by an abusive person, this can prevent the abusive person from being able to see or listen to the survivor.

Seek Support from IoT Manufacturers

Survivors may want to communicate with the companies that build or run their IoT devices, to let them know about the abuse. The company may be able to provide suggestions and to help institute protections. For example, it may be possible to add security or block the abusive person's devices or locations, preventing them from accessing to a device or account. This may not always be possible and may not be the best option for preparing evidence for court, but survivors should decide what would be the best solution for their own situation.

IMPORTANT: Be sure to help the survivor to make a safety plan, in case removing access escalates an abusive person's behavior. Refer victims to a local advocate who understands tech safety, or let them know about the resources in our Survivor Toolkit at TechSafety.org.

Carefully Consider Use of IoT Devices

Because IoT devices can give a large amount of access to private spaces, people should carefully consider their own needs and weigh the potential risks and benefits of using IoT devices. A survivor may decide that the practical benefit of using an IoT device outweighs the possible threat of abuse. Some survivors may decide to temporarily take a break or entirely give up IoT devices until they feel safe to use them. We do not recommend telling survivors to get rid of IoT, but instead believe that a thoughtful conversation about the pros and cons can help survivors to weigh their needs and risks.

Provide Support

If a survivor feels that IoT devices are being misused, they should be supported in trusting their instincts. Many survivors have people telling them that their experiences are not real or that their instincts are wrong. Sometimes it can be useful to let them know that IoT devices can be used to cause harm and that they should document what is happening to them.

Next Steps in your Investigation

Proving technology abuse can be challenging, however it *is* possible to successfully prove tech abuse cases through effective investigation and creative advocacy. For more information, see the resources in our Evidence Collection Series.

If you have further questions about investigating tech abuse cases, please contact Safety Net, and visit TechSafety.org for more information.

Special thank you to Bryan Franke of 2CSolutions for providing expertise and guidance on the creation of this series.

Supported by US DOJ-OVW Grant No. 2016-TA-AX-K069. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of DOJ. We update our materials frequently. Please visit TechSafety.org for the latest version of this and other materials.

NNEDV

Evidence Collection Series:
Messages & Messaging Platforms

Where to begin?

This guide is a part of a series that details how to collect evidence related to the misuse of technology in domestic violence, sexual assault, and stalking cases. Before proceeding, we recommend that you read A Primer for Using the Legal Systems Toolkit: Understanding & Investigating Tech Misuse, Approaches to Evidence Collection: Survivor Considerations, and Approaches to Evidence Collection: Civil vs. Criminal Systems.

Who should use this resource?

The series is part of a Legal Systems Toolkit that includes various detailed guides meant to assist prosecutors, law enforcement, and civil attorneys.

IMPORTANT TIP/NOTICE FOR ADVOCATES: If you are a non-attorney survivor advocate, we strongly recommend that you do NOT gather or store evidence for survivors. You can greatly assist survivors by giving the survivor the skills to gather the evidence themselves. Your participation in the process of gathering or storing evidence can lead to you being forced to testify in court, which can undermine confidentiality protections, and negatively impact both the survivor and the integrity of your program. If you have questions, please contact Safety Net.

Messaging: An Introduction

For survivors of domestic violence, sexual assault, and stalking, messaging platforms can serve as a lifeline because information can be communicated to help without risk of being overheard. However, abusive partners can also misuse messaging to harass, intimidate, and threaten. We will outline the differences between criminal and civil investigations of messaging evidence, identifying what evidence to look for, where to search for it, how to gather it, and how to locate corroborating evidence.

Messaging: The Technology

“Messaging platforms” can describe a variety of communication technologies. We use the term to include both text and instant messages sent from built in or native applications such as SMS and MMS, instant messaging applications built into devices such as Apple’s iMessage, and instant messaging apps that a user must download onto their device, like WhatsApp.

Text and instant messaging platforms have many overlapping functions and features, but also some important differences. Both can send and receive different types of information including text; photo, video, and audio content; emojis and other interactive images; and files and hyperlinks.

Text messages are generally sent from one mobile phone to another over a cellular network. Phone companies commonly retain information related to sending or receiving these messages, although the actual substance of the message--including text, images, and videos--are only kept for a very short period of time, if at all. Text messaging tools are generally provided as basic or “native” feature of a mobile device and no apps need to be downloaded in order to access messages. While not universally true, generally, the substance of a message is only accessible on the sending and receiving devices and does not automatically sync across multiple devices, unless a user specifically sets it up to do so.

Instant messages are sent over the Internet or cellular-data networks, and many services also allow users to communicate through video and audio calls. Information is held by the instant messaging company rather than the cellular company. Retention policies vary across companies, and not all companies save message content. Some services, like Snapchat, automatically delete messages soon after they are read by the receiver, although there still may be circumstances where deleted information may be retrieved.

Many instant messaging platforms are not pre-installed on a device, but instead must be downloaded through an app store. However, Apple now pre-installs iMessage on their devices, which allows communication between Apple devices. Most instant messaging services can be set up to automatically sync across multiple devices and a number allow for messages to be sent from multiple locations, including from devices and online portals.

Messaging Evidence: The Digital Trail

Many cases often lack documentary evidence or witnesses, and a court's ruling is often determined exclusively by whether a person's testimony is believed. Messaging evidence can strengthen cases by providing proof of abuse and a clearer picture of relationship dynamics. While messaging evidence can be extremely useful, it is not always properly sought out or collected, can get accidentally deleted or tainted.

TIP ABOUT MESSAGING AND PRIVACY: Many people have hundreds or even thousands of pages of messaging conversations. Most information will not be relevant to the case and to ensure survivor privacy, read only what is relevant. Prosecutors and law enforcement will want to limit the amount of messaging evidence collected, to protect against turning over unnecessary information due to *Brady* requirements. Turning over a victim's private messaging information that is not directly relevant to the case can impact the willingness of victims to testify, confuse the factfinder(s), and can lead to unnecessary re-traumatization.

Identify All Platforms Used

Communication usually happens over a variety of platforms over times. It is best to start interviews with broad questions about how communication took place throughout the relationship.

Follow up with specific questions about whether there was communication via text messaging, social media networks, messaging apps within email applications like Google Hangouts and Yahoo Messenger, apps that delete messages after they've been read like Snapchat, or other messaging apps common in your area, including Skype, WhatsApp, Viber, and Signal.

Protect the Data

Messaging apps can be accessed remotely by an abusive person through an insecure password or automatic syncing, so important evidence could be modified or deleted if not properly protected. Discuss password safety and the importance of changing passwords on all relevant platforms and devices. If survivors have any concern their device(s) may be infected with spyware, plan how to change passwords without alerting the abusive party and consider how to gather evidence of spyware.

It is also important to identify if messaging information is being synced across devices or backed up to the cloud. Survivors may not know that their private information is on the cloud or that another person can access it. The abusive person may be able to modify or remotely wipe device information if a backup cloud storage is used, so changing the password and disconnecting other devices from the account may be essential.

Help Survivors Document Evidence

It is common for survivors to collect evidence themselves through the use of screenshots, photographs and video footage. Help survivors understand what information to retain and how to capture evidence. Letting survivors know to include the contact information of the sender, the date and time stamp, and the entire conversation so that important contextual elements are included, can help to ensure the usefulness of the evidence. Read more about the importance of involving survivors in the process of collecting evidence.

Messaging Evidence Collection

There are several categories of evidence that should be considered for evidence.

Evidence the survivor has access to

After taking steps to protect against accidental or malicious destruction of evidence, identify what messaging evidence the survivor can access. While this evidence may not always be admissible, it will give a better picture of the case and of what other evidence needs to be sought.

Start with the device, while also protecting the survivor's rights and privacy. Next, look at online accounts connected to the messaging platforms. By identifying what information is available in a survivor's online accounts, you can help them strategize about how to protect that information and determine what additional steps need to be taken to ensure the evidence will be admissible.

Many companies have options for users to download all information associated with their account. These functions allow a survivor to get a large amount of information about what has transpired on their accounts. It may be necessary to use a legal process, like a subpoena, court order or search warrant, for the information to be admissible in court.

Finally, ask survivors if there are other people who may have supporting evidence. Sometimes survivors use other people's devices or accounts to communicate, and they may have sent screenshots to friends or family. Those sent messages could be a way to access destroyed information or may identify an important witness. This information may also be valuable to show the survivor's state of mind at the time of the communication.

IMPORTANT NOTE ON SPOOFING: Spoofing, or falsifying a caller ID to disguise identity, is a commonly misused technology. Abusive parties can also use it to falsify evidence or attempt to paint survivors in a negative light. It's important to be aware of spoofing and to be prepared to help the court understand how it can be misused. Read more in our Spoofing Evidence Collection guide.

Evidence that the Abusive Party has Access to

The abusive party, if they have access, may attempt to delete or add to the conversation in order to make the survivor look bad. Identifying information the other party can access will help protect evidence. It can be hard to disprove this information while in court, so the sooner you can identify the discrepancy, the better. This is also why it is important to consider collecting digital evidence from the devices used by both the survivor and the abuser (if available), and then to compare that data.

Evidence that Needs to be Obtained by Court Order or Subpoena

Although the survivor may have access to evidence on their devices and online accounts, not all of that evidence is necessarily admissible. Certified copies may be necessary to support the accuracy of evidence. At times, survivors only have partial evidence and it may be necessary to seek the full information through legal process. For example, a survivor might have taken screenshots of a few text messages, capturing what they deemed to be the best evidence, but it doesn't capture the entire conversation. By subpoenaing telephone records to show the times that messages were sent or received, you may help to convince a court that the survivor's evidence should be taken seriously.

Phone and instant messaging companies are generally required to comply with properly executed criminal court subpoenas, court orders, and search warrants. This includes responding to requests about evidence from the accounts of the survivor *and* the person accused of abuse.

Most phone companies do not store the actual content of a text message for long, if at all. They generally only retain information showing the time a text message was sent or received. Even properly submitted legal process (i.e. subpoena or warrant) will not get the actual content of a text message unless done quickly. Additional information may be available through a warrant, though may be limited due to these retention policies.

IMPORTANT TIP ABOUT PRESERVING DATA: Preservation requests are essential to accessing important information, especially considering retention policies. Preservation demands are particularly important for law enforcement, although civil preservation letters may also be useful.

Similarly, retention policies vary greatly between instant messaging companies. Some companies may retain information, while others, such as Snapchat and WhatsApp, rarely do. If you want to learn more about a platform's retention policy, run an online search with the following phrase "[Platform name] information retention policies."

Differences Between Civil and Criminal Investigation

While survivors will be important resources in all case types, the evidence available may differ in criminal versus civil investigations. Approaches to Evidence Collection: Civil vs. Criminal Systems discusses important differences in the two systems and offers tips for professionals in each system.

Tips for Collecting and Maintaining Messaging Evidence

TIP 1: Obtain the Entire Conversation

Many survivors will bring copies of an offending message rather than the entire conversation. Be clear about what you need from the beginning. Some courts will not accept partial messaging conversations. You never want to lose the ability to introduce important messaging evidence just because you do not have an entire conversation, especially if the remainder of the conversation has no negative impact on the survivor's case.

TIP 2: Get Supporting Evidence

A screenshot of a message may be adequate for many courts. However, this type of evidence may not always be sufficient. Best practice is to obtain supporting evidence, which could be in the form of telephone records that show the date and time that messages were sent or received, which can be compared with the screenshot. Be creative, there may be a variety of ways to support the evidence through other documents, witnesses, and the client's own testimony. Forensic examination may also provide more information, including whether a message has been modified, altered, or deleted.

TIP 3: Sender Information

Survivors frequently will have the abusive person’s name in their contacts and therefore the sender is identified by name rather than a phone number. Because any name can be assigned in a contact list and connect to any number, this can be an issue in court cases. It may be beneficial to delete the person’s name from the contact list before taking screenshots so that the number shows up, instead of the name.

Another option is to include a screenshot of the contact entry along with the messages to demonstrate that the contact entry name is connected to that number. With this option, you will also need to provide evidence that the screenshots of the entry and the messages were taken contemporaneously.

TIP 4: Time and Date Matter

Many messaging platforms hide the exact time that messages are sent or received, but most devices provide easy tricks to show a time stamp. On an iPhone and many Androids, swiping from the right side of the phone towards the left side while holding your finger on the screen will show the timestamp on a message. Because technology changes, do an online search for “How to show time stamp on messages on [device name]” if you’re unsure how to access that.

Collecting evidence with time and date stamps can be useful for painting context of the case. It can show that somebody sent 15 messages in a minute or two, which is substantially different than 15 messages in a day or two. They can also be useful because they can be cross referenced with phone records to help prove whether evidence was tampered with, or whether protection order violations have occurred.

Next Steps in your Investigation

Despite challenges of technology evidence, it *is* possible to successfully prove tech abuse cases through effective investigation and creative advocacy.

For more information, see the resources in our Collecting Evidence Series. Further information on how to admit messaging evidence can be found in How to Gather

Technology Evidence for Court from the National Center for Juvenile and Family Court Judges. If you have further questions about investigating tech abuse cases, please contact Safety Net, and visit TechSafety.org for more information.

Special thank you to Bryan Franke of 2CSolutions for providing expertise and guidance on the creation of this series.

Supported by US DOJ-OVW Grant No. 2016-TA-AX-K069. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of DOJ. We update our materials frequently. Please visit TechSafety.org for the latest version of this and other materials.

Evidence Collection Series:
Spoofing Calls and Messages

Where to begin?

This guide is part of a series that details how to collect evidence related to the misuse of technology in domestic violence, sexual assault, and stalking cases. Before proceeding, we recommend that you read A Primer for Using the Legal Systems Toolkit: Understanding & Investigating Tech Misuse, Approaches to Evidence Collection: Survivor Considerations, and Approaches to Evidence Collection: Criminal vs. Civil Systems.

Who should use this resource?

The series is part of a Legal Systems Toolkit that includes guides to assist prosecutors, law enforcement, and civil attorneys.

IMPORTANT TIP/NOTICE FOR ADVOCATES: If you are a non-attorney survivor advocate, we strongly recommend that you do NOT gather or store evidence for survivors. You can greatly assist survivors by giving the survivor the skills to gather the evidence themselves. Your participation in the process of gathering or storing evidence can lead to you being forced to testify in court, which can undermine confidentiality protections, and negatively impact both the survivor and the integrity of your program. If you have questions, please contact Safety Net.

Spoofing: An Introduction

Spoofing, often called “caller ID spoofing,” disguises a person’s true name or number. Text messages, e-mail, phone calls and other forms of electronic communication can all be spoofed. This resource provides information on how spoofing is commonly misused and how to gather evidence for court.

Spoofing: The Technology

Understanding how spoofing works can help guide evidence collection and safety planning. Spoofing can be done through mobile apps, websites, forwarding services, or a combination of technologies. Below are some of the most common technologies to consider when looking for spoofing evidence.

Services Designed for Spoofing

SpoofTel, BluffMyCall, SpoofCard, My Phone Robot, Covert Calling, and Spoof My Phone are just a few of the numerous spoofing services and apps.[1] These services often vary in how they function. Some companies allow spoofing messages and calls through an internet connection, while "prepaid calling services" generally rely on traditional phone service providers. Some require the creation of an account to use the service, which may require the user's actual phone number or other personal information, while others do not. Services can be free or for purchase. The user can usually choose what number they want to appear on the receiver's device and some allow users to use a variety of different numbers.

Other Services Misused for Spoofing

Other services and apps that can be misused for spoofing include Google Voice, Grasshopper, MightyCall, DingTone, Telzio, Freedompop, Voiceably, OnSIP, and Vonage.[2] These technologies are mainly created for professionals whose work benefits from using "fake" numbers. While they don't have the same negative stigma as spoofing services, an abusive person can still misuse them. Unlike spoofing companies, these services usually give the user a reusable, unique number rather than allowing them to use a variety of different numbers or to select another person's number to mimic.

Spoofing: Tool of Domestic Violence, Sexual Assault, and Stalking

Below are *some* potential ways that abusers and perpetrators misuse spoofing:

1) **Hiding Identity:** Abusers may misuse spoofing to make it harder to prove abusive behavior or to make it easier to gain access when the victim is trying to avoid contact. Some services allow the user to change how their voice

[1] http://www.crunchytricks.com/2017/01/free-unlimited-spoof-calling.html

[2] https://getvoip.com/blog/2016/10/10/google-voice-alternatives/.

sounds or to mimic specific numbers to pretend to be somebody the survivor may communicate with.

2) **Getting Personal Information:** An abusive person may misuse spoofing to contact someone the survivor knows in order to trick them into disclosing the survivor's location, schedule, or other sensitive information.
3) **Harassing,Intimidating, By-Passing Safety Planning Stategies:** Spoofing can also be used to show a trusted contact name or number, to trick survivors into viewing or accepting abusive communication from their abuser.

Spoofing: Evidence Collection

The following information distinguishes between evidence collection in criminal and civil spoofing cases, including what evidence to look for, where it can be located, and how to gather additional supporting evidence.

Tips for Getting Survivors Involved in Evidence Collection

Help survivors understand how to protect, collect, and preserve evidence. Survivors' active participation can lead to information that may strengthen the case, and can give survivors essential tools for safety and healing regardless of the outcome of the case.

IS SPOOFING ILLEGAL? It depends. The Federal Communication Commission (FCC) makes it illegal to spoof in order to defraud, cause harm, or wrongly obtain anything of value.[3] These laws are generally designed to protect consumers, mainly referring to monetary damages. There are no federal or state spoofing laws that are designed to specifically address spoofing in the context of domestic violence, sexual assault, or stalking. However, other existing laws can be successfully used to hold perpetrators accountable. For example, spoofing could lead to a criminal or civil case under existing laws against harassment, stalking, or cyberstalking. Legal protections will vary depending on the state. For more information about laws in your state, visit WomensLaw.org.

[3] https://www.fcc.gov/consumers/guides/spoofing-and-caller-id.

Types of Spoofing Evidence

Although locating spoofing evidence may be challenging, both direct and circumstantial evidence can be gathered to prove a spoofing case.

Direct Evidence: Records to Prove Spoofing

The easiest process to prove calling or messaging spoofing in many cases is to compare the phone records of both parties, looking at what calls are listed on the abusers bill that were made around the time the survivor received the spoofed call. These may point to a spoofing service being used, but this is not a foolproof method. The abusive person may have used a different phone or various spoofing services, and/or may have communicated via WiFi, instead of their personal cellular, home, or work phone.

Phone records are not the only tangible records that can assist in proving spoofing. For example, if a company requires the user to pay for the service, then obtaining the abusive person's billing records may reveal evidence. If a service requires WiFi access, it may be possible to obtain data from the abusive person's WiFi network or Internet Service Provider (ISP). These forms of evidence are frequently accessible in criminal investigations, but may be more limited in civil cases.

Spoofing Relay Evidence

Some companies provide a unique, random number that can be used to "relay" a call or text to the victim's number in various way, while others allow the user to enter a number they want to appear. The most common method is for a person to call a company that offers the relaying service and then enter the number they wish to call. The service provider then automatically calls the number, but the number that shows up on the recipient's caller ID does not belong to the original caller. A person can also send a text message through relay by using forwarding services. Proving relay spoofing may require accessing records for both parties or a forensic analysis of devices.

App or Web-based Spoofing Evidence

Many spoofing services are available as apps or are accessible through a spoofing website. Apps and websites generally will not show up in phone records or on the abusive person's device call or text logs. Additionally, a forensic analysis of the device may not uncover spoofing logs or records because of how apps store (and protect) information on devices. Obtaining access to web browsing history may also prove the use of a spoofing website. Similarly, records of app downloads or usage may provide useful evidence. If an app or website has been used, collecting evidence will often require obtaining records from the company.

Information Requests to Spoofing Companies

If the investigation can narrow the list of possible services misused, subpoenas can be sent to a handful of identified companies in an attempt to see if any respond with helpful information. Some companies are paid with a credit or debit card. Seeking out these financial records can be an effective way to start the investigation. Additionally, some perpetrators may have used spoofing in the past against other people, while still with the survivor. Ask the survivor if they ever witnessed this behavior. If they have, ask what they remember about how the abuser did it and what devices and apps they may have used. If the survivor still has a computer the abuser used while in a relationship, consideration should be given to searching this device with consideration for the laws of your state. This also applies to old smartphones left behind that were used by the abusive person.

Try Discovery

Although not all companies will respond to information requests, particularly in civil cases, it is still worthwhile to seek discovery whenever possible. A court may order that relevant information be exchanged via discovery. For example, in some case types, such as divorces, it is common to exchange financial information like credit card statements. Additionally, courts may allow for more expansive discovery where records are directly related to an important factor in the case, such as the well-being of children.

IMPORTANT NOTE ON RELATED STATE LAWS: State laws vary. Some courts routinely order both parties to bring phone records and some states preclude discovery without permission of the court. It is important to research the laws and practice within your jurisdiction and to seek local assistance.

Differences Between Civil and Criminal Investigation

While the survivor's story will be an important resources in all case types, the other evidence available may differ in criminal versus civil investigations. Approaches to Evidence Collection: Criminal vs. Civil Cases discusses important differences in the two systems and offers tips for professionals in each system.

Circumstantial Evidence: Looking for Spoofing Clues

Even when records are available, it is useful to seek out circumstantial evidence to help the court better understand how spoofing impacts the survivor and to clearly demonstrate when and how spoofing has occurred.

IMPORTANT NOTE ON SAVING EVIDENCE: Digital evidence is frequently deleted. Let the survivor know *early* of the importance of saving information and how to appropriately collect and store digital evidence.

Look for Patterns

Spoofing may happen repeatedly and within an identifiable pattern. See if the communications take place on a schedule or in a way that is similar to past communications. For example, if calls always start after 6:30 pm, and it can be shown that the abuser works until 6:00 pm daily, or if the survivor routinely received calls from the abusive person at 5:00 am, and are now receiving spoofed calls around that time. Pay attention to details related to when the abusive person calls and texts versus when they do not. The smaller the timeframe, the better. Getting the victim to start a log can be a useful way to get them involved in the investigation and can prove helpful in identifying possible patterns.

Look for Similar Information

Similar mannerisms, words, and information can serve as a type of digital fingerprint. Calls and texts from a number that is known to belong to the abusive person, or review of other past communications like emails or social media posts, can be compared to the spoofed communication for possible clues. A common phrase, misspelled words, or unique punctuation are all biproducts of a person's personality and pattern of behavior and can be used as one more piece of evidence to connect the spoofed communication(s) to a specific person.

Additionally, proof of other types of online stalking or cyber abuse, even if not contemporaneous, could be used as supporting evidence. Many abusers have used similar tactics in the past against multiple victims. Evidence of other types of technological intrusion involving other victims may not always be admissible, but can help paint a picture and unveil areas for further investigation.

Look for Correlating Life Events

Demonstrating that a breakup, child custody changes, modifications to court orders, or some other noteworthy event took place around the time that the spoofing started or increased can be persuasive. Phone records or other messaging logs can be particularly helpful to prove the timing of the spoofing with any changes or events in the victim's life.

Consider Other Types of Abuse that Occur at a Similar Time

Domestic violence, sexual assault, and stalking is often a combination of various abuse tactics. Connecting the spoofing to other actions taken by the abusive person, within a similar timeframe, can help to show that spoofing was likely a part of the overall abusive behavior. Showing other acts can also help to show a pattern of abuse, which may be necessary in order to prove certain crimes like stalking.

Consider Impact on Survivor

While a strong spoofing case relies on tangible evidence, a victim-centered approach also looks to the ways spoofing impacts a survivor's life and well-being. Continuous calls and messages from unknown or misleading numbers, and the fear of constantly being harassed or stalked by an abusive person can psychologically traumatize a person. Some potential effects of spoofing on the survivor include self-isolation due to fear, paranoid thoughts, poor performance at work, emotional breakdowns, and depression. If the victim has a strong reason to believe that the abusive person has used spoofing against them, then it may be helpful in court to show how their health and quality of life have diminished following the spoofing incidents. With their permission and with careful consideration to consequences, admitting relevant health records, or other connected personal details coinciding with the timing of the spoofing, could be supporting evidence.

Steps to Support Victim Safety & Privacy

Gathering evidence to use in court may be an important step towards ending spoofing. However, the primary goal of many survivors may be to immediately stop the abusive behavior, even if it means that the evidence will be lost. Below are safety suggestions that can be used before or after gathering evidence.

Seek Support from Communication Providers

Phone companies may provide suggestions and help institute protections if they are informed about the spoofing. For example, it may be possible to only permit calls from known numbers or to require individuals to state their name before the call can start. This may not always be possible and may not be the best option for obtaining evidence for court, but survivors should decide what would emotionally and practically be the best solution for them.

Remain Alert

It is important to empower survivors to trust their instincts. Many survivors have people telling them that their experiences are not real or that their instincts are wrong. Support can help them know that it is okay to block a number, ignore a random text, or not to pick up a phone call until they find a more permanent solution. Sometimes it can be useful to just let survivors know that they can feel free to hang up or to verify the caller before giving out information.

Strengthen Evidence Gathering

Sometimes the best way to get evidence is through the court. Once in court, the survivor or their legal team can let the court know what is happening and request an opportunity to request evidence from the other party.

Use Court Action to Deter Abuse

The act of going to court can be an effective way to end the abusive behavior. Obtaining a court order and ensuring that all orders are properly served can alert the abusive person that their actions have consequences. In some situations, the possibility of a lawsuit can be enough to get the behavior to stop.[4] However, the abuser could also escalate abusive behavior, so appropriate safety planning should be addressed prior to taking this step. Remember the survivor knows the abuser better than anyone else and will be an invaluable resource in this process.

Specify Needs in Protective Order

Ask the court for an order that specifically states that the abusive person is not to communicate or attempt to communicate with the survivor from their number or any other number and that they are not allowed to request a third-party to make that communication on their behalf. Specific provision will make it easier to hold the abusive person responsible for violations. The formal threat of further legal action *may* also push the abusive person to change their behavior.

To assist in drafting impactful orders, sample language is below. Of course, it is important to consider the rules, laws and procedures in your jurisdiction.

SAMPLE PROTECTIVE ORDER LANGUAGE

“Refrain from communication or any other contact, either directly or through a third party, by mail, telephone, e-mail, voice-mail, social media, online forums, or other electronic or any other means with [survivor]. Respondent must refrain from using, or directing another person to use on their behalf, any service, app, or

[4] https://www.fcc.gov/consumers/guides/spoofing-and-caller-id

website which hides the Respondent’s identity (also known as spoofing) in order to communicate or contact the Petitioner. Respondent shall not make any of the above communication with any individual, place, business, or institution connected to the Petitioner unless the communication is required for a purpose completely unrelated to the Petitioner. Spoofing includes any attempt or act of disguising one’s digital identity using any service or technology that allows for falsifying one’s name, number, etc. ‘Disguising the identity’ includes but is not limited to the act of changing one’s voice, using a false number, impersonating another individual, mimicking another person’s number, lying about one’s true identity, or otherwise disguising one’s digital identity using any service or technology.”

Change Phone Number(s)

Survivors may choose to change their number to limit the abusive person’s ability to communicate with them through spoofing. Before recommending this step, it is important to consider safety. Changing a number can make it difficult to collect evidence and could escalate the abusive persons’ behavior. It could also lead to isolation, and the loss of much needed support, or impact employment, schooling or other services. Survivors should be given information to help weigh the benefits and drawbacks of any safety strategy, including changing numbers. As an alternative, help identify resources that might allow them to get a new number, while also retaining the original number for evidence gathering. A pre-paid phone or a call relaying services, as discussed previously, are some options.

Other Considerations:

It is not uncommon for other violations to occur at or around the same time as the spoofing. Note whether the abusive person has access to any previously unknown details about the survivor. Do they now have knowledge about a change or event in the survivor’s life that they would have not known before? Obtaining information inappropriately is a major safety concern and possibly a new criminal act. It can also indicate that a false identity or other misuse may have been used to obtain the information, so efforts should be made to investigate this as well.

Next Steps in your Investigation

Despite challenges, it *is* possible to successfully prove tech abuse cases through effective investigation and creative advocacy. For more information, see the other resources in our Collecting Evidence Series. If you have further questions about investigating tech abuse cases, please contact Safety Net, and visit TechSafety.org for more information.

Special thank you to Bryan Franke of 2CSolutions for providing expertise and guidance on the creation of this series.

Supported by US DOJ-OVW Grant No. 2016-TA-AX-K069. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of DOJ. We update our materials frequently. Please visit TechSafety.org for the latest version of this and other materials.

Evidence Collection Series:
Mobile Spyware

Where to begin?

This guide is a part of a series that details how to collect evidence related to the misuse of technology in domestic violence, sexual assault, and stalking cases. Before proceeding, we recommend that you read A Primer for Using the Legal Systems Toolkit: Understanding & Investigating Tech Misuse, Approaches to Evidence Collection: Survivor Considerations, and Approaches to Evidence Collection: Criminal vs. Civil Systems.

Who should use this resource?

The series is part of a Legal Systems Toolkit that includes guides to assist prosecutors, law enforcement, and civil attorneys.

IMPORTANT TIP/NOTICE FOR ADVOCATES: If you are a non-attorney survivor advocate, we strongly recommend that you do NOT gather or store evidence for survivors. You can greatly assist survivors by giving the survivor the skills to gather the evidence themselves. Your participation in the process of gathering or storing evidence can lead to you being forced to testify in court, which can undermine confidentiality protections, and negatively impact both the survivor and the integrity of your program. If you have questions, please contact Safety Net.

Spyware: An Introduction

Mobile devices hold intimate details of our lives and this single access point for information is usually a convenience. But for survivors of domestic violence, sexual violence, or stalking, an abusive person can misuse spyware to access a terrifying amount of information.

This document includes information about how to identify a spyware case, how and where to look for evidence of spyware, and tips for gathering evidence.

Spyware: The Technology

"Spyware" refers to software applications that give a person remote access to a device, allowing them to monitor and collect information and device activity. To install spyware on a mobile device, a person generally must have physical access to the device, or convince the user to install the software, often through deception. For Apple products, devices will generally need to be jailbroken before these applications can be installed. While the Play Store for Androids does not allow applications to run covertly, the Android operating system does not enforce this requirement and spyware can be installed.

Dual-Use Applications and Tools That Can be Misused

In addition to spyware applications that have a main purpose of remotely spying on someone, there are also applications that have legitimate purposes, but can be misused to access a device remotely or receive data from it. Dual-use applications may be purposefully downloaded by the user and they may not even be aware the abusive person has remote access to their device data through it. For example, the Find My Friends or Find My iPhone applications on iPhones can be used to surreptitiously track a user.

There are also many applications with secondary *features* that share location data. For example, if certain settings are used, Snapchat or Google Maps may be misused to access the location information of someone's device. Depending on what information the abusive person knows, it may be helpful to assess for the misuse of these types of apps as well.

Analyzing Spyware Cases

Though the use of spyware in domestic violence, sexual violence, and stalking cases has been well-documented for almost two-decades—first with computers and now with mobile devices—the methods used to monitor and collect information about survivors are often complex and may or may not include spyware. It can be useful to start an investigation by considering all possible sources –including non-spyware options—for how an abusive person could be inappropriately obtaining information.

Step 1 – Give the survivor the benefit of the doubt.

When a survivor is concerned that an abusive person knows too much information about them, tell them to trust their instincts. Ask about what information the abusive person seems to know and help them document behaviors and events to see if there is a pattern. For example, the abusive person might show up at places the same time as the survivor or may drop hints that they are collecting information about the survivor. In one case, a survivor was looking at a particular pair of shoes online and shortly after the abusive person sent the survivor the exact URL and said they would look great on her. Hints, however, are not always so blatant. It is important to walk through experiences that have caused the survivor concern.

Step 2 – Identify what information the abusive person is accessing.

Identify each piece of information that the abusive person appears to have access to. For instance, if the abusive person consistently shows up at the survivor's work, despite varying shift times, there may be a leak in the survivor's workplace (i.e. a coworker) or the online scheduling software, or maybe the schedule is emailed to an account that is being monitored. If the survivor has gone to three different grocery stores and the abusive person has shown up each time, the abusive person may be accessing their real-time location through GPS.

Step 3 – Consider social explanations.

The most common, non-technological explanation for an abusive person having too much information about a survivor is a friend or relative leaking the information. Friends or relatives might not understand the entire situation, and may unwittingly provide information. Alternatively, someone may be spying on the survivor and purposefully reporting to the abusive person.

Ask the survivor if any friends or relatives were privy to the information in question. Then, from that list of people, ask if any of them are or could be in contact with the abusive person. If so, the survivor may need to tell them to stop sharing information, or the survivor may need to stop sharing information with them.

Step 4 – Consider everyday features and apps that contain the information.
An abusive person may inappropriately access information by misusing everyday features and apps used by the survivor. For example, they may know or have guessed a password or be physically looking through phone activity while the survivor's phone is unattended.

Ask the survivor where each piece of information may be stored. Is the work schedule in their email? Does the abusive person have access to the Find My iPhone feature? Knowing where the information is located will help narrow the focus in determining how the abusive person is getting the information.

Step 5 – Consider information the survivor shares publicly.
Some survivors may unwittingly share private information through publicly accessible accounts, including social media. For example, they may have posted about their work shifts and not realized the privacy setting was set to public.

It is important to understand what the survivor chooses to share about themselves and how. An online search for the survivor can be helpful. Identify what social media platforms are used and then identify what information is accessible or visible to the general public. They may be posting publicly, rather than privately or the abusive person may be connected to a third-party who can see that activity. Help survivors review privacy settings so they can make informed choices about who has access to their information.

Step 6 – Look for evidence of spyware.
If no other leaks of information can be identified or if the abusive person knows too much without explanations, look for evidence of spyware.

IMPORTANT: If you believe the survivor is being targeted by spyware, one of the safest things the survivor can do is use the phone as though nothing is wrong. Normal use will avoid tipping off the abusive person of suspicions, allowing more time to collect evidence before it is destroyed. It is important to speak with survivors about the pros and cons of this strategy, as well as strategies to use their devices in more secure ways. Some people may feel safest getting rid of the device or doing a factory reset to try to rid of the spyware.

Preparing to Gather Spyware Evidence

Often, domestic violence, sexual assault, and stalking cases lack documentary evidence or witnesses, and cases are determined by which person's testimony is believed by the courts. Evidence of spyware misuse can clearly demonstrate how the abusive person created an environment of fear and control.

Unfortunately, useful evidence is not always properly sought out, is accidentally deleted, or is not collected properly. Below, we will describe how to collect and maintain evidence to increase its usefulness in court. You can also read about the differences in technology evidence collection between criminal and civil cases.

IMPORTANT: Be sure to help the survivor to make a safety plan, in case the abusive person's behavior escalates in the course of the investigation. Refer victims to a local advocate who understands tech safety, or let them know about the resources in our Survivor Toolkit at TechSafety.org.

Identify Types of Evidence

The existence of spyware can be difficult to uncover as the application may be hidden or may not clearly disrupt the regular use of the device. It can be especially difficult to prove the misuse of dual-use applications because it must be shown that the application is present and that it is being manipulated to obtain remote access to device data without the survivor's knowledge or permission, or with coerced permission.

Protect all of the mobile device's data.
In some cases, direct evidence of spyware on a mobile device can only be obtained with the help of a forensic professional. It is important to protect all data since you may not know immediately what to look for and it may be needed later by a forensic professional.

Throughout your investigation and evidence collection process, help the survivor build a picture of what leads them to believe spyware is being used. They may have seen a receipt for a spyware company on the abusive person's computer or the survivor may have information that the abusive person used this type of software against another person. Even without this information, asking open ended questions may encourage a survivor to share information that may help the investigation.

NOTE ABOUT PASSWORDS: Usually when technology is used to facilitate abuse, it is a good idea to help the survivor to change their passwords and to disconnect other devices from accounts. However, if spyware is on the device, it is not safe to change passwords on that device. Create a plan on how to change passwords without alerting the abusive person, such as using a separate, safer device. Once a plan is created, you can help the survivor create strong passwords.

Create a list of information that will help the case.
You may not know all the experiences that have led the survivor to believe the abusive person has access to information, which limits your knowledge of what experiences are relevant. The survivor may not be familiar with the justice system and may be unaware of what is most important for court. Have a detailed conversation with the survivor, and encourage them to share as much detail about the situation as they can remember. It is also important to be very clear about what kind of information you are seeking.

Help the survivor understand how to protect, collect, and preserve digital evidence. Read more about the importance of involving survivors in the process of collecting evidence. Survivors' active participation can lead to information that may strengthen the case, and can give survivors essential tools for safety and healing regardless of the outcome of the case.

Next Steps in your Investigation

Spyware misuse is one of the most invasive forms of tech abuse, and investigations can be extremely complicated. However, it *is* possible to successfully prove spyware cases through effective investigation and creative advocacy. For more information, see the resources in our Collecting Evidence Series. If you have further questions about investigating tech abuse cases, please contact Safety Net, and visit TechSafety.org for more information.

Additional Resources

- Spyware, Surveillance, and Safety for Survivors
- 12 Tips on Cell Phone Safety and Privacy
- Technology Safety Quick Tips
- Admissibility of Forensic Cell Phone Evidence
- How to Gather Technology Evidence for Court from the National Center for Juvenile and Family Court Judges
- Avoiding Cell Phone Spyware Infestation
- Vice, Motherboard: When Spies Come Home Series
- How to Protect Yourself from Creepy, Phone Snooping Spyware
- How To Bust Your Boss Or Loved One For Installing Spyware On Your Phone

Special thank you to Bryan Franke of 2CSolutions for providing expertise and guidance on the creation of this series.

Supported by US DOJ-OVW Grant# 2016-TA-AX-K069. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of DOJ. We update our materials frequently. Please visit TechSafety.org for the latest version of this and other materials.

NNEDV

Approaches to Evidence Collection: Survivor Considerations

The civil and criminal legal systems play a pivotal role in protecting victims and holding offenders accountable in cases involving domestic violence, sexual assault, and stalking. While documentary evidence and other witnesses play important roles in many cases, the most important evidence in many cases is the survivor's story. When victims feel believed and that they can trust the officer or attorney, they're more likely to provide important evidence (especially in cases where the evidence may include sensitive or embarrassing content).

This document will provide suggestions for evidence collection, with a particular focus on getting survivors involved in the evidence collection process. For more detailed suggestions on investigating evidence, take a look at our guides for investigating specific types of evidence.

IMPORTANT TIP/NOTICE FOR ADVOCATES: If you are a non-attorney survivor advocate, we strongly recommend that you do NOT gather or store evidence for survivors. You can greatly assist survivors by giving the survivor the skills to gather the evidence themselves. Your participation in the process of gathering or storing evidence can lead to you being forced to testify in court, which can undermine confidentiality protections, and negatively impact both the survivor and the integrity of your program. If you have questions, please contact Safety Net.

Evidence Collection

Technology evidence can generally be found from three different sources:

1. Evidence the survivor has access to, including evidence on the device and evidence that can be accessed through online accounts.
2. Evidence from the abusive person, whether it is shared with the survivor or the abusive person has exclusive access.
3. Evidence that needs to be obtained by court order or subpoena.

Evidence the Survivor Can Access

Survivors often have access to a large amount of evidence of tech misuse. Many survivors will have received (and saved) harassing messages and other proof of abuse. In addition to the evidence that the survivor may have collected or retained, there may be evidence on a survivor's device(s) and accounts that can be useful. While not all of this evidence will be admissible into court, getting a full account of available evidence will give a better understanding of the case and of what other evidence needs to be sought.

One of the richest sources of evidence is the survivor's devices. While many survivors will be willing to hand over devices for examination, it is essential that survivors are informed about information that will be required and collected in the investigation before examining device(s) and accounts. Domestic violence, sexual assault, and stalking often impact a survivor's sense of control over their information and their world. The information in question may have a direct impact on the survivor's safety, and is necessary in making safety plans. They also have a right to control their privacy to the greatest degree possible within the investigation.

Evidence from the Abusive Person

Technology evidence may be most effectively obtained through access to the abusive person's device(s) or accounts. Some criminal investigations may be able to access the devices and accounts for the accused perpetrator, but civil cases may have a difficult time obtaining this information. In some cases it will be possible to analyze the abusive person's accounts and devices, while in other cases it may be necessary to seek out the information in other ways.

One useful way of obtaining evidence from the abusive person's device(s) and accounts is through the discovery process. Some civil cases do not allow for formal discovery, but the court will allow for requests for the parties to share any information they intent to present to the court. Discovery requests can help you obtain information that can lead to important evidence, such as call and message history, images, bank statements, IP address, download history, and other digital records.

While the evidence may ultimately come from the abusive person, survivors often have useful information about what evidence may be available on the perpetrator's accounts or devices. It is important to bring survivors into the investigation whenever possible.

Evidence that Needs to be Obtained by Court Order or Subpoena
Although the survivor may have access to some evidence, they may only have partial or incomplete information, and either way not all of the survivor's evidence will be admissible. It may be necessary to seek out information from other sources in order to support the accuracy and admissibility of the evidence. Subpoenas, or other court orders, may be sent to companies that hold data relating to the survivor or the abusive person, for example phone companies, social networks, and software or app providers.

There are several limitations to getting available information with subpoenas. For example, retention policies vary greatly amongst companies, including length of time and the content that they retain. Some companies may retain transactions (e.g. that an email message was received or sent) while others retain the actual content of the communications. It is often possible to locate information about retention policies by identifying a specific platform and doing an online search with the following phrase "[company name] and information retention policies."

If a court order or subpoena is necessary to obtain information it is a good idea to take steps to ensure that the information is not prematurely deleted by the company. Preservation letters can help to ensure that the information is available when proper legal actions seeking the information has been sent.

Before taking the steps of seeking out information through a court order or subpoena, it is worthwhile to ask how the evidence is going to be used. Not all useful evidence needs to be admitted into court. Perhaps the evidence can be used to negotiate a settlement or a plea? If so, obtaining a certified copy through a court order or subpoena may not be necessary. A survivor's screenshot may be sufficient. If you are hoping to introduce the evidence into court, you may need to obtain a subpoena, a warrant, or a certified copy.

IMPORTANT NOTE ABOUT AGREEMENTS: Frequently, parties will consent to technology evidence being admitted into court. It can be useful to consider communicating with the other side (if possible) about whether an agreement can be reached regarding introducing certain evidence. It is far easier to introduce the evidence by agreement than to seek out a legal process or fight about the issue in trial.

Tips for Getting Survivors Involved in Evidence Collection

A survivor's story is generally the most important evidence they can provide, however, many survivors can also be of assistance throughout the entire case, including evidence collection. The following suggestions can increase the role of survivors in helping to obtain evidence, including identifying evidence from the abusive person, and evidence that needs to be obtained through a court order or subpoena.

Step 1: Identify all technology used

It is best to start interviews with broad questions about how technology played a role throughout the relationship, including communication, whether the abusive person had access to the survivor's device(s) or accounts, and any technology-related abusive behavior or information that the abusive person had that concerns the survivor. Follow up with specific questions about different technologies and experiences.

Meeting with law enforcement or an attorney can be stressful, which can impact memory. Additionally, survivors may not know what information to share, or may be concerned about giving access to embarrassing information. It can be helpful to familiarize yourself with common technology, because survivors may need you to jog their memory or help them to understand what might be relevant.

Step 2: Protect the data

It is important to protect all data since you may not know initially what to look for, and a forensic professional may need to examine devices or accounts for evidence of abuse or unauthorized access.

Cloud-based accounts are commonly connected to many devices, automatically syncing information across several devices or backing up data. Help the survivor to identify what cloud-based accounts are linked to their device(s), and, if possible, which accounts the abusive person may have access to. Remote access not only allows an abusive person to see private information, but could also enable them to remotely destroy evidence.

After identifying data that is in the cloud or accessible online, it is important to discuss options for protecting that data. This might include blocking the abusive person's access to accounts. Let the survivor know the benefits of password security and the importance of changing their passwords on all relevant platforms and devices.

If the survivor has any concern that their device(s) may be infected with spyware, it is important to first create a plan on how to change passwords without alerting the abusive person. Once a plan to avoid detection is created, you can help the survivor create strong passwords. There are also specific safety concerns when using iCloud.

IMPORTANT: Be sure to help the survivor to make a safety plan, in case the abusive person's behavior escalates in the course of the investigation. Refer victims to a local advocate who understands tech safety, or let them know about the resources in our Survivor Toolkit at TechSafety.org

Evidence can also be lost through normal device and account functioning. In an effort to increase the speed and usability of devices, many companies set up devices and accounts to automatically delete information. Ask the survivor if their device or account is set up to automatically delete messages. Most people will need to check the device and account settings to confirm.

Digital evidence can also be compromised if a device is lost, stolen, or broken. Because accidents happen, plan early for how to backup evidence.

Step 3: Teach the survivor what information will help the case

As the investigator, you are not a part of the conversations between the parties, which limits your knowledge of what conversations are relevant. The survivor knows their situation best, however due to a lack of familiarity with the justice system, they may be unaware of what is most important for court. Both parties lack a crucial piece of information and, as part of a survivor-centered investigation, it is important to clearly identify what you need the survivor to look for and share.

Step 4: Explain how to document the evidence

There are several ways to document digital evidence. Forensic professionals are regularly used by police departments, district attorneys' offices, and in high-cost litigation. It is less common for forensic professionals to be used in civil cases. In cases where forensic professionals are not available, it is common for survivors to collect evidence themselves by taking screenshots or printing out evidence. Explain to the survivor what information to retain and how to document instances when technology is used to abuse or stalk.

Make sure the survivor knows what they need to do, or not do, so that they don't accidentally do something that will negatively impact the collection process. Backing up the information in multiple places is also suggested as long as that can be done safely.

SURVIVORS' RIGHT TO TECHNOLOGY: Telling a victim to get rid of their technology or to go offline is not a feasible option. Technology has become a necessity in our everyday lives, and it can also serve as important lifeline for victims in an emergency. Survivors may need to remain online to decrease isolation, for their job, or as a part of custody planning. Telling a survivor to get rid of an account or device may even escalate the level of violence since an offender may then seek the victim out in person.

Next Steps & Additional Resources

Proving technology abuse can be challenging. Despite the challenge, it *is* possible to successfully prove tech abuse cases through effective investigation and creative advocacy.

This document is a part of a series that details how to collect evidence related to the misuse of technology in domestic violence, sexual assault, and stalking cases. We recommend that you also read A Primer for Using the Legal Systems Toolkit: Understanding & Investigating Tech Misuse and Approaches to Evidence Collection: Civil vs. Criminal Systems. The series is part of a Legal Systems Toolkit that includes guides to assist prosecutors, law enforcement, and civil attorneys.

If you have further questions about investigating tech abuse cases, please contact Safety Net, and visit TechSafety.org for more information.

Supported by US DOJ-OVW Grant No. 2016-TA-AX-K069. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of DOJ. We update our materials frequently. Please visit TechSafety.org for the latest version of this and other materials.

NNEDV

A Primer for Using the Legal Systems Toolkit: Understanding & Investigating Tech Misuse

The Legal Systems Toolkit helps legal system stakeholders: Law Enforcement, Attorneys, Court Personnel, Community Corrections Officers, and others identify privacy and safety options, what technology is relevant to a case, and how to use technology evidence to hold offenders accountable. Before reviewing the toolkit, there are several important considerations that serve as a starting point for your work.

Technology Isn’t the Problem

Regardless of the tactics, abusive behavior will always be the core issue. Technology misuse is one tactic among many that offenders use against victims. Even if technology was removed from the equation, the abuse would likely continue in other ways. Technology *does* extend the reach of a perpetrator, and it can increase the trauma for a victim. However, it can also provide a rich trail of evidence and can be used strategically in safety planning.

A Survivor’s Right to Technology

Telling a victim to get rid of their technology or to go offline is not a feasible option. Technology has become a necessity in our everyday lives, and it can also serve as important lifeline for victims in an emergency. Survivors may need to remain online to decrease isolation, for their job, or as a part of custody planning. Telling a survivor to get rid of an account or device may even escalate the level of violence since an offender may then seek the victim out in person.

People working in legal systems have a unique opportunity to help victims stay connected, document the abuse, and safely access tools that can help in an emergency. Refer victims to a local advocate who understands tech safety, or let them know about the resources in our Survivor Toolkit at TechSafety.org.

Establishing Rapport

In cases involving domestic violence, sexual assault, stalking, and harassment, legal system stakeholders play a pivotal role in protecting the victim and holding the offender accountable. Establishing rapport with the victim is incredibly important to the investigation and evidence collection process. When victims feel believed and that they can trust the officer or attorney, they're more likely to reach out with new evidence, or when things get worse (especially in cases where the evidence may include sensitive or embarrassing content).

The Digital Trail

Technology evidence may provide law enforcement and attorneys with tangible proof needed to make a case. It may also help in negotiating pleas, settlements, obtaining confessions or guilty verdicts, or relieve some of the pressure on victims to testify against their perpetrator. Technology evidence may include devices, messages, pictures or videos, account logs or billing statements, apps, location information, and "metadata" or the information embedded in emails.

Evidence Collection Tips

1. Some victims have an idea of what technology is being misused, while others may only know that offender knows too much about their conversations, whereabouts, or activities. The questions you ask can help narrow down the technology being misused.
2. In addition to obvious evidence like threatening text messages or social media posts, also consider hidden cameras, location trackers, mobile device apps and settings, or spyware, which are all becoming more common.
3. Remember that how-to videos and blogs provide tutorials and make misuse easier, even for those with little or no technology expertise.
4. Know the specific language technology companies require in warrants and orders to ensure that you are gathering the information you need.

5. Although technology can produce an enormous amount of available evidence, it's important to balance the amount collected with the victim's privacy rights and needs of the case, especially considering discovery rules.

Consider All Possible Charges

There is a wide array of laws that can be used to hold offenders accountable. Be sure to identify and consider both state and federal laws that:

- address violence and abuse,
- explicitly or implicitly include the use of electronic communications, or
- relate to technology, communications, privacy and confidentiality, even if they are not necessarily focused on domestic violence or sexual assault.

If an incident may not be a crime or legal offense itself, see if a larger pattern of behavior could fall under a stalking or harassment statute.

In one case, the victim and an officer realized, by using a documentation log, that messages were sent while the abuser was at work. The behavior was also caught through work surveillance cameras and computer logs.

Building a Case & Working with Victims

- Help victims learn to safely document incidents to establish a pattern and identify possible evidence.
- Send preservation requests to ensure that evidence is not deleted.
- Refer victims to an advocate for information on increasing safety.
- Share information about the limitations of the evidence or the law. When victims know more, they're empowered. And when they feel listened to and respected, they are more likely to trust you with new information or come to you when the situation gets worse.

Supported by US DOJ-OVW Grant 2016-TA-AX-K069 (Technology Abuse & Safety Project). Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of DOJ.

We update our materials frequently. Please visit TechSafety.org for the latest version of this and other materials.