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

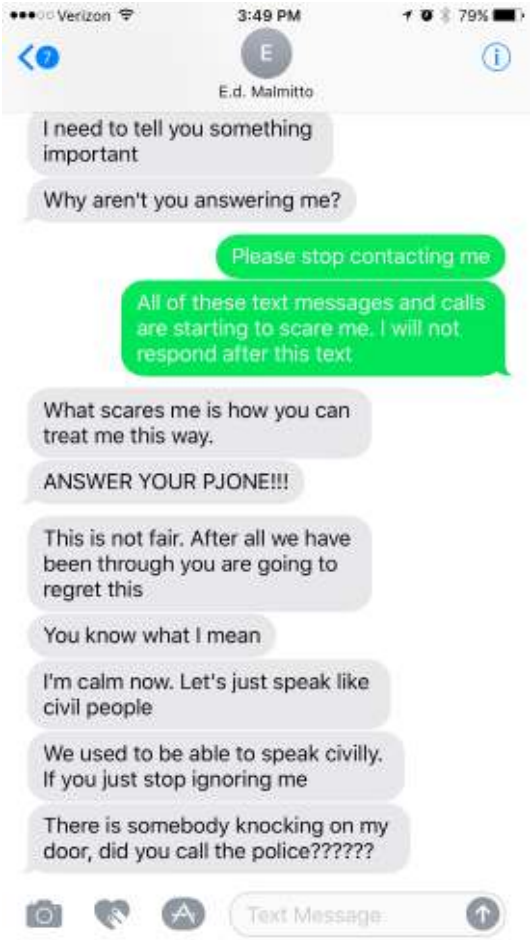
CELEBRATING 80 YEARS 1937-2017

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:



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]."

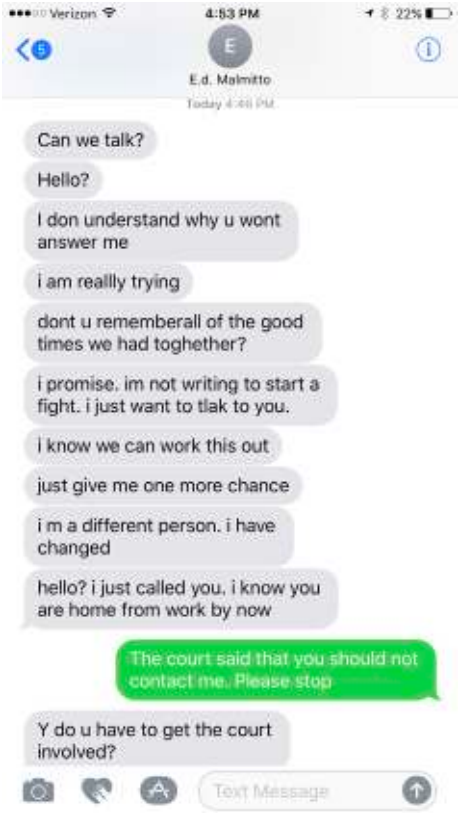
What Should You Capture?

On Your Smartphone

TEXT MESSAGES

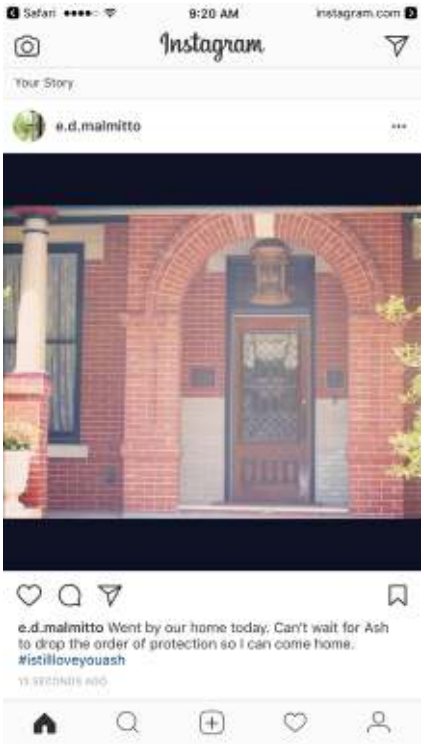
- The abusive message, including other text messages that give context to the abusive message.
- The time and date the message was sent. Some message apps can be tricky and hide the time and date. You may need to tap or swipe on the message to show the date and time it was sent. If you aren't sure how 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.

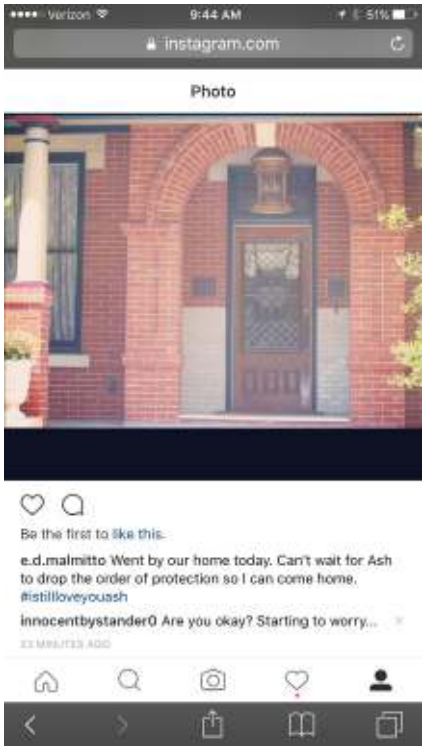


INSTAGRAM

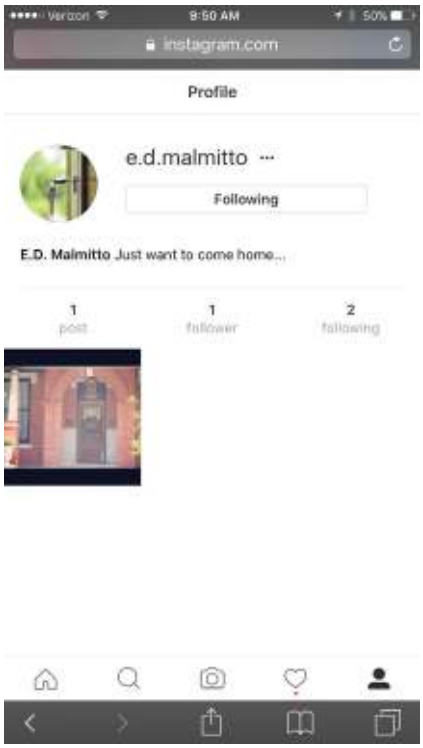
- If it is the Instagram image that is harassing, capture the picture and who posted it. The name of whoever posted the picture will show up above the picture.



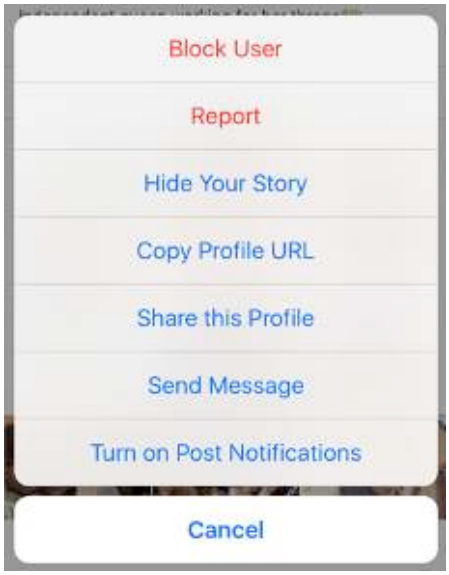
- The comments. If the abuse or harassment was in the comment section, take a picture or video of the username, the image, and the comment. At the bottom of the comment, it will show when the person made the comment. Document the date that you took the image or video.



- 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.



- 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

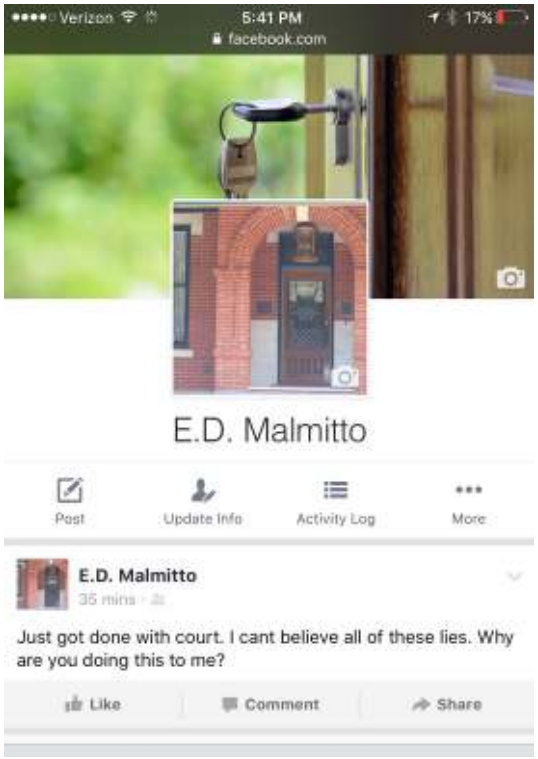
- The email message. You can print out the email, which will show the To, From, Date, and Subject information. A printed email will also show the file name of any attachments. When printing an email, it can change how the email looks and that can make it harder to get the email admitted into court. If 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

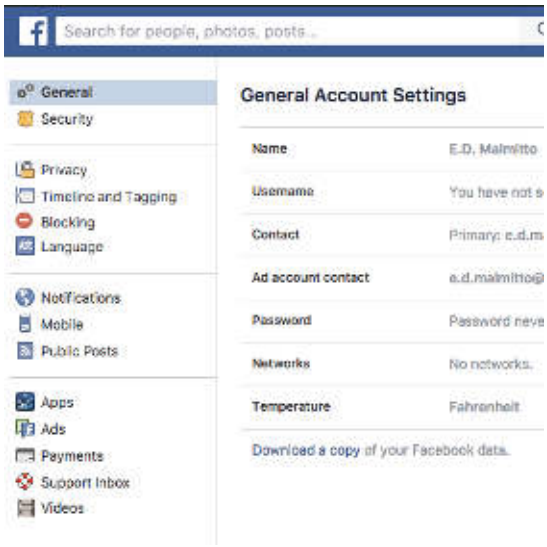
To capture evidence from Facebook, here's what you'll need:

- 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.



- 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.



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.

- 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.

- 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