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.