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.

© 2018 National Network to End Domestic Violence, Safety Net Project.
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.