

Expert Q&A

Topic: Technology, Social Media, and Victim Safety

Moderator: Jason Adams

Host: Erica L. Olsen, M.S.W.

Date: June 20, 2018

Length: 1 hour

What strategies can survivors use to preserve evidence from social media?

There are many ways to capture evidence of harassment, threats, or other abuse happening on social media. One of the easiest ways is to take a screenshot on a phone or a computer. We have an instructional video on how to take a screenshot on our website, but you can also Google “how to take a screenshot on...” and type in whatever type of phone or device you have. NNEDV (National Network to End Domestic Violence) also collaborated with the National Council of Juvenile and Family Court Judges to produce a document entitled “[How to Gather Technology Abuse Evidence for Court](#),” which gives step-by-step guidance to capture a variety of different types of social media evidence. You can contact us if you want the link to this handout.

There are a few things that are important to note about collecting evidence. For example, if the platform is Snapchat, the sender of the message will get a notification if a screenshot is taken of the message. It’s also important for survivors to have conversations with an advocate, attorney, and/or law enforcement to ensure that they are collecting evidence in a format that will be accessible and admissible in court.

There are also some built-in features in some social media platforms, such as Facebook’s DYI, which stands for Download Your Information. This feature allows users to download their entire Facebook history and would preserve any posts. If a survivor starts this process after receiving harassing messages, it can save the content even if the abusive person deletes it later.

It’s also important for survivors to plan around preserving evidence and reporting content. If something is reported and it does violate the platform’s terms of service, then it will be removed completely, so it’s important for the person to capture that evidence prior to submitting the report.

Are there apps that survivors can use to increase their safety?

A few years ago, we launched our [App Safety Center](#)—you can find that at TechSafety.org—to help survivors navigate the huge and ever-growing world of apps being created for them. There are many apps available for various purposes and with any of them, we would highly encourage survivors to fully understand the app and think through all the pros and cons before relying on one, especially in the case of an emergency. We encourage this because, unfortunately, many of the apps we tested did not work exactly like they said they would, and many had serious limitations to them. Some did not share location information when they said they did, and others sent wrong information. Some also pose pretty serious privacy and safety risks. The apps meant for survivors are usually either informative apps, screening apps, or emergency apps. The informative apps usually do not collect any personally identifiable

information, but it's still important for the survivor to consider the privacy they have over the device they want to access the app on. If the abuser may be accessing the phone or looking through it, seeing an informative app about abuse and how to access help may escalate their abuse. The emergency apps—those that contact emergency services or friends/family—often have very different features. It's important for a survivor to look at their options and consider what they need the app to do. Do they want an easy way to contact police? Or a local friend? Do they only want an option for capturing any abuse or assault to collect evidence? Or is the person just trying to put a plan in place in case they don't return from a jog in the park? These are all things that different apps or different features of apps address. Please check out the App Safety Center, we have lists of considerations, suggestions for app developers, and information about various available apps. We also tested and reviewed many more than are actually on the site, so please contact us if you have questions about one that is not listed. Also, NNEDV is currently working on creating an app to assist individuals in collecting digital evidence of abuse. It will be released next year.

How can we use technology to serve victims?

First and foremost, it's critical that we always think through our use of technology to ensure that nothing we do creates a risk to the safety and privacy of survivors. This is important because while there is always an urge to look at the newest technology to enhance our work, the regular everyday technology we use is still changing and can create serious risks if we're not careful. We use phones, computers, and email regularly to communicate with each other or other service providers. My voicemail is now a very different system than it used to be—I can get my voicemails via email, and on my Mac they open automatically and save on my computer unless I specifically go in and permanently delete them. If I'm someone who has regular phone contact with survivors, this could create a real privacy risk (which could easily be a safety risk). Even our copy machines are dramatically different, usually saving a copy of everything run through the machine to the hard drive. When we lease those and give them back with the hard drive intact, who gets access to millions of documents with survivor's personally identifying information? So, to answer the question directly, we can FIRST ensure that we are using technology with safety and privacy in mind. And we can harness technology to help with that. Copiers can have an additional feature that doesn't allow documents to be saved. We can also choose to use newer, more secure forms of communication with survivors. [Resource Connect](#) is currently the only chat and text platform that we know of specifically designed for victim service providers that uses zero-knowledge encryption—meaning no one would have access to the content of the conversations except the survivor and the program, not even the host providing the platform. Another online service, Gruveo, allows individuals to have a private video call without the need for downloading software onto a computer or creating a login. These features can be important if the survivor is using a computer or device that the abuser may also have access to. There are also many ways that we can harness social media to increase awareness and engage our communities, although they are not platforms built for having really private conversations. Overall, we should constantly be engaging in a process to critique the various ways we use all types of technology to see how we can increase privacy, safety, and awareness.

What advice do you share with victims regarding the use of social media? Should they use it cautiously or not at all?

We are fierce advocates for a survivor's right to use technology and online platforms in the ways that they want to. Just as we think survivors shouldn't have to change jobs because an abuser is harassing them in the workplace, we also think accountability for online harassment should be placed with the abuser. Social media can be an important part of a survivor's life. Some people are required to have accounts for their work. Others find it to be the only way to stay connected to family and friends—which is such an important thing when abusers have tried to isolate you. What is really important is that survivors feel informed in how they use social media so they can make decisions on which platforms to use and how. Most of the major social media platforms have several options for controlling privacy and security (important: these are two separate things—privacy is controlling who sees your content and security is controlling who has access to your account). It can actually be a lot easier to control who sees your information on a social media platform than controlling who could access your identifying information when you give your phone number and address to retailers when shopping. It's important that we provide information to survivors so they can increase their privacy and security to use platforms as safely as possible. We absolutely believe that we should not be telling survivors not to use certain platforms but instead providing information about privacy and security options and potential risks. If survivors just stop talking with us about their use of social media, then we can't effectively help to safety plan around it.

What are some best practices for staying safe online?

- Use strong passwords. This sounds so simple, yet research shows over and over again that the vast majority of people are using very weak passwords. We have to remember that we now need to use passwords that computers can't guess. The longer the better. It doesn't even have to be so complex that you can't remember it. Test various passwords out on howsecureismypassword.net. When I put in a simple word with some letters swapped out for numbers, it says a computer can guess that in less than a day. But if I enter the password "youshallnotpass" it says it'll take a computer a thousand years to crack that. That's what you want.
- Don't use the same photos for social media accounts or generally anything online that you don't want connected. Images can be searched, and if you have different accounts with different names, maybe so your employer won't find your wild social media posts, but you use the same profile photo, those accounts can easily be connected.
- USE SECURITY SETTINGS!! Control access to your account. Use two-factor authentication. If you're not sure what that means, look it up—that's your homework.
- We have a ton of suggestions and tips on online privacy and security in our [Survivor Toolkit](#) on our TechSafety.org site, so please check that out for more info.

How can victims identify apps that may have been placed on their phone to track them?

As I mentioned earlier, survivors can look through all the downloaded apps on their phone to see if there is something running that they are not familiar with, and they can also call their carrier and ask if any location tracking options have been activated. Most of the third party family location sharing apps, which should be visible on the phone, require both phones to have the app and to be connected. If the abuser has installed spyware on the phone and is using that to track location, that will be very difficult to detect without law enforcement involvement to do a scan of the phone. Most of the time, survivors who think this may be the tactic being misused believe so based on what the abuser knows and seems to have access to.

How can you protect your cell number from being spoofed? And how can you prove that your number was spoofed in court?

There is no way to stop your number from being spoofed. For those who are not familiar, spoofing is the process of falsifying or faking the phone number that shows up on someone's caller ID. Abusers misuse spoofing services to trick survivors into answering calls or pretending to be someone that they are not. Many services also allow the person to change their voice so the fake calls can actually be quite convincing. We have heard several examples of survivors getting a call from the court saying their court date is rescheduled when it's really not. Then they don't show up, but the abuser does.

Under the Truth in Caller ID Act, the Federal Communications Commission prohibits a person from falsifying caller ID information with the intent to defraud or cause harm. Proving your number was spoofed is fairly easy since your phone records will not show an outgoing call at the time that someone's phone received a call that appears to be from your number. Proving that an abuser has spoofed a number as a tactic of harassment or abuse will require access to their phone records, which will show them calling a number associated with a Spoofing service, and/or their device, which can show if they used a spoofing app. If you believe that spoofing is being misused by an abuser, you can definitely reach out to our team to help think through and plan a response.

Is there a way to recover evidence, such as text messages and images that have been deleted off of a victim's phone or computer?

Most devices, including phones, tablets, and computers, only immediately delete content from your view and only permanently delete content if the user chooses that option or if space is needed on the device. You can often access folders on the phone for recently deleted content. You can Google your specific device and the question "how do I recover deleted images" for information and steps. There have also been many cases where law enforcement recovered deleted content and used that to hold an abuser accountable.

What is the best way to stay abreast of the most recent and prevalent ways victim safety is being jeopardized by technology?

First, talk to survivors about their tech use and the ways they communicate with the abuser and their family/friends. We have often learned of a newer technology that an abuser is misusing because a survivor has told us what was happening, even if they didn't know the name of it or how it works (example: deleted emails).

Second, pay attention to tech in general. We do a lot of work to learn about technology and stay informed about emerging privacy and safety risks. The challenge to this is that we need to really critique and analyze technology and how it works to apply it to this work and identify how it could impact survivors or be misused as a tactic of abuse. It is important to try technologies and platforms out to learn them so that we can have conversations with survivors, answer their questions, and help them increase their privacy and safety. But it's hard to know it all, so focus on things that are coming up frequently with the people you are working with. And look to us for information so you're not recreating the wheel. We are constantly adding to the content in our toolkits and posting blogs about emerging tech or privacy and safety issues. So, look to others to supplement what you're doing and help you respond effectively to the needs of survivors.

In your experience, what changes have you seen in social media, good or bad, relating to victims' safety?

Most major platforms have made pretty significant changes over the years and mostly for the better. A few examples of this are:

- Most of the major social media companies now have pretty active safety advisory boards, and we are a part of many of them. As a member of some of those, I can definitely say that many products have been altered or canceled altogether based on the feedback of members.
- Several companies have been putting a lot of resources into building larger teams to respond, in many languages, to harassment and abuse. We have also seen some of the new staff purposely being hired from victim services because they want people who really know this work and how to communicate with survivors appropriately.
- Snapchat recently introduced an in-app reporting feature and Facebook reinstated its reporting feature within Messenger, responding to requests for users to be able to report harassing messages easily.
- All major social media platforms have created policies on the distribution of nonconsensual intimate images so that survivors can get content taken down quickly.
- Many platforms have also significantly streamlined their law enforcement request processes.

Generally, there are still ways that many platforms can be improved and can enhance the ability to respond to harassment and abuse happening on the platforms, but we are definitely seeing a commitment and a process for continuing to get better, which is not the case with many serious privacy and safety issues that exist for survivors today, particularly around how data are collected offline and then shared without the knowledge or consent of the person.

Has there been any leeway in implementing laws to protect against cyberstalking and harassment?

There is actually a bit of a misconception that exists with the idea that more laws are needed to address the ways that technology is misused. In many ways, technology misuse is already covered by existing laws. First, stalking and harassment laws already include language around electronic communication. Second, many laws are not actually specific to a device or platform, but to the abusive behavior—harassment, impersonation, etc. Third, there are a ton of laws that can often apply depending on what is happening and what the abuser is doing. They may have violated privacy laws, trespassed to hide an eavesdropping device, or misused access to data at work as part of their tactics. That said, there are still some gaps, but they are pretty specific. One challenge is making sure that courts are open to assessing technology-facilitated abuse as falling under these existing state criminal laws and protections. For example, some judges may be looking for very traditional violations of certain laws, such as an identity theft violation to include stealing someone's Social Security number and creating financial accounts in a person's name; however, there may be instances where an abuser creating a fake email or social media account to act as the victim could fall under the state's identity theft laws.

Are there specific laws pertaining to stalking and social media bullying?

Yes. Federal and state stalking laws include language that will apply to social media platforms. Again, this is because it's often about the behaviors and not the specific mode of communication. Repeated, unwanted, and harassing messages sent via a social media platform can definitely be part of a pattern of stalking. Our WomensLaw.org website provides great information on state-specific laws and has an [entire section on technology](#) misuse and laws, so I would check that out to learn more about your specific state laws that can apply to various forms of technology abuse.

What is the best application a parent can use to follow or access a teenager's social media or texts?

Our work focuses on spy apps and increasing privacy and safety around social media, but we don't encourage people to use stealth spy products to monitor their children or anyone else. Many spyware products, like mSpy, require the phone be jailbroken or rooted to use most of the features, including social media monitoring. This significantly increases the vulnerability of the phone to hackers, viruses, and malware, and is not something that should be done to a child's phone if the goal is to protect them, their privacy, and their devices.

There is a difference between being honest with a child about using parental control apps and surreptitious stealth spy monitoring of a child. This is particularly important for us to understand as advocates, because stealth spy monitoring of kids and teenagers sends a message that monitoring devices and accounts is an okay behavior. This can lead to confusion over who should be allowed to monitor their devices and accounts. The reasons of a concerned parent don't sound very different from the reasons given by an abusive ("concerned") partner who is pressuring them to share their account information. As advocates, we need to recognize that confusing message/modeling and encourage parents to talk openly with their kids—to develop a trusting and supportive environment, give their kids the ability to have a private world and a space to explore and create their identity without being constantly monitored by their parents.

It is also extremely likely that if a parent is using stealth spyware to monitor a child/teenager, they will soon reveal to the child that they know information that could only be garnered by spying on them; thereby letting them know that they are monitoring it. This breaks any semblance of trust between the child and the parent, and leaves the child feeling isolated and not able to go to parents for support when trying to figure out how to negotiate genuine risks they may encounter. It can also leave them unable to form close bonds with others because it interferes with the way they build relationships. So, in order to promote healthy boundaries, privacy, safety, and a space where kids will talk to their parents about anything bad that may be happening online, we suggest either not monitoring and instead working to establish a trusting relationship around online activity, or at a minimum, being upfront about any monitoring (which removes the need for the service to be operating without notice to the person). Giving kids opportunities to be trusted and to take risks helps them find their own way through life, even if it means they make mistakes. It's about educating them and supporting them in understanding how to safely navigate their way on social media and other forms of mobile and online communication.

Additionally, we've often found that people are asking these questions about children who are often technically too young to be on many of the online platforms in the first place, according to the rules of those platforms. We cannot encourage the monitoring of children in certain spaces when being in them is a violation of the rules of the platform. Allowing them to be in those spaces essentially encourages them to violate those terms of use, which are set up as a way to increase privacy and safety. For example, we've seen parents allow their kids to lie about their age on Facebook, but that platform is built so that kids under a certain age have an entirely different experience than older people using it (can't get friend requests from strangers, etc.). Using these built-in tools can be more effective as a way of preventing danger or risks. So, communicating with children about when and how to use certain platforms becomes the most important piece.