NNEDV

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 <u>or any other number</u> 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.