SAFETY CONSIDERATIONS FOR CO-PARENTING AND VISITATION APPS

techsafety.org.au

Please note that the contents of this document should not be regarded as legal advice. The information contained within is relevant as of February 2025.

Why This Topic?

In recent years, co-parenting and visitation apps have become increasingly popular as a tool for divorced or separated parents to communicate about issues related to their children. Parents may choose to use such an app voluntarily, or in some cases, courts may order parents to communicate with each other through an app about custody-related matters. This is especially common in situations where abuse has been perpetrated or has occurred within the relationship. Some of these apps have features that allow courts to monitor all communications, which helps provide documentation of compliance with court orders. It's important to consider the implications for safety, privacy, and confidentiality when using these types of communication apps.

This document is split into two sections: information for those using the apps and information for those assigning or interfacing with them in a professional capacity. While these apps may provide a platform for individuals (the parties to the case) to communicate, and for court personnel such as judges, legal professionals working with survivors, and supervised visitation providers to monitor, it is vital that all audiences are aware of how these apps function and the potential risks they may pose to the users/survivors.

Considerations for Survivor Privacy and Safety

When are communication apps appropriate?

Privacy is important and deeply connected to safety in situations where there may be abuse or stalking. A parent who is unable to use a co-parenting app safely may have difficulty complying with the court's requirements. The purpose of the court's orders is to further the well-being of the child, which cannot be accomplished by inadvertently endangering a parent. For example, in situations where there has been abuse in the relationship, consider a scenario in which personal information shared through the app – such as schedules, contact information, or details about the child's activities – can be misused to stalk, harass, manipulate, and exert power and control over the survivor. This can in turn cause stress to the parent and also have a negative impact on the child's well-being.

Assessing for privacy concerns that could be relevant to the use of communication apps is an important step prior to their use. Below are some of the questions that can help with this assessment.

Is the privacy notice legible and useful?

An app's privacy notice is the public-facing document that informs users of how their data is collected and handled. Privacy notices allow users to make an informed decision about whether they would like to add their sensitive data into an app or an account. Unfortunately, privacy notices can be difficult for most people to read and comprehend. The app's privacy notice should be written in plain language. Ideally, it should clearly describe:

1. What permissions it requires from the device (location services, camera access, etc.).
2. What data it collects.
3. With whom it may share what data.
4. How the company will handle the data.
5. What policies the company has regarding data retention and deletion.

Are consent requests and user permissions transparent?

Sometimes when an app or website asks whether a user consents to giving it certain permissions or information, it is not upfront about what it is asking for or it may use deceptive tactics to get users to agree to give it certain permissions. An example of this would be a prompt to a user to give an app permission to collect location data, that has the "Yes" box checked by default and does not state whether it will share that location data.

Other issues could also exist in the overall design of apps that collect more identifying information about the users than the users could be aware of. Understanding exactly what the app and the company behind it is collecting is an important step in ensuring appropriate usage, especially for cases where privacy is connected to safety.

Does the app require location features to be enabled?

Safety experts commonly recommend that survivors turn off a device's GPS and other location settings when they are not in use. This is to avoid abusers misusing GPS information to locate the survivor. Apps that ask users to keep their location settings on at all times conflict with this best practice.

Some features of a co-parenting app may require location services to be enabled for documentation purposes. For example, the app may document whether a parent was at a specific location at a specific time so that the other parent could pick the child up. However, these situations cover only a small fraction of a parent's life or parenting. An app feature that prompts a user to upload a location at a scheduled time presents more safety options than an app that requires location to be constantly on.

Is it a mobile app, a web portal, or both?

Some apps can only be used through a phone or tablet. Others also (or only) have a web portal that allows users to log in from any device that has a browser. Since not everyone has a smartphone or a tablet, it is important to know whether an app requires one before issuing a court order or making a recommendation. Beyond this issue of accessibility, there are also survivor safety considerations.

In addition, it is not always safe for survivors to use their own phones or tablets. Abusers or stalkers may have installed stalkerware on them, which could allow the abusive person/stalker to see all the survivor's activity in the app (including any passwords or financial information entered into it). If the abusive person and a survivor are not currently living separately, or live near each other, the abusive person may also still have physical access to the survivor's mobile devices. If an app has a web portal, a survivor without a safe mobile device can use an alternate device, such as a friend's or family member's computer or a library computer, to interact with the app. For security reasons, it is important that an app with a web portal supports password protection.

The other side of this coin is that if a survivor's mobile device is safe for them to use, but the abuser may know or be able to guess their account passwords, the web portal may introduce a vulnerability for the survivor (since the abusive person could access their account from anywhere). Because of this, it is preferable that any co-parenting or supervised visitation app supports some form of multi-factor authentication. Multi-factor authentication means that in addition to a password, someone who logs into an account must provide at least one other "factor." This might be a code texted or emailed to the person logging in, verification through an authenticator app, a facial recognition scan, or something else. Since it is a security best practice, this also protects information intended for the court's purposes of monitoring compliance, from hackers.

As discussed above, greater flexibility – in this case, an app with both a mobile version and a web portal – tends to be an asset for survivors. It allows them to use the options that are safest for them. However, as also discussed above, it is also important for all supported options to have proper security.

What metadata is on images and videos?

Metadata is "data about data." It may also be called the "Properties" or "Info" of the file, depending on the operating system. Let's say a parent takes a photo of their child with a digital device. The data is the photo's image stored as file information (such as a .JPG file). The kinds of metadata of that photo that are included as file properties will depend on the capabilities of the digital device that was used. Metadata may include the date and time the photo was taken, the location at which the photo was taken (if the device was a smartphone), the name or some user ID of the person who owns the device or a related account, information about the device, and more. There are numerous online tools that remove metadata. If a court is considering ordering an app and is not clear on its metadata policy, the court could also consider suggesting one of these third-party tools.

What permissions does the app require?

Apps require certain "permissions" to be able to function. This could be for a core functionality of the app, or for an optional feature. Some examples that could occur in co-parenting and visitation apps:

- The app could request permission to access the device's microphone so that a parent can record a voice message for a child.
- The app could request permission to access the device's location in order to document that a parent arrived at a required location at a specified time.
- An app may request permission to access the device's camera for a virtual visitation session. If the user denies this permission, they will not be able to

appear on video during a meeting.

- There may also be different levels of permissions. For instance, a user might grant an app access to a device's location all the time, or only while using the app, or they may refuse it permission entirely.

Some of these permissions could reveal sensitive information about a survivor. If you are considering ordering co-parents to use a particular app, you should find out whether it has responsible permissions practices. This may include rethinking the court's own needs as well, in order to limit collection of data that could affect a survivor's safety if compromised. The court's purpose in ordering such apps is monitoring compliance with the court's orders – what does the court truly need for this purpose? If a survivor is ordered to use an app that will not allow them to take the safety measures they discussed with a DFV practitioner or other domestic violence professional, they may become confused.

What data does the app/web portal collect? Who is it shared with?

In general, apps and software systems should only collect the data that they need to function. If they do not collect the data, it cannot be breached or shared. In the case of an app meant to document co-parent communications, the needed data will necessarily be more than for some other types of apps. However, courts should still consider whether the apps are collecting unnecessary data. For instance, if the app is a mechanism for the parties to communicate, it does not necessarily need to collect and store user phone numbers or home addresses. It should also not need to collect information about device usage unrelated to the app.

In addition, there is the question of who else may be able to see the data. Most software systems have a tech stack, meaning that they use other tech products as pieces within their own. This is analogous to, for example, a carpenter using bricks, boards, and pipes that were made by others, rather than having to make all their own materials from scratch. Are other tech companies whose products are part of an app or website's tech stack able to access the developer's user data in readable form? Along with the tech stack, many apps and websites share data with, or sell it to, advertising partners. If a developer of a co-parenting/visitation app does this, it could mean that people far beyond the court are able to access the data of the people using the app. It is often possible to view what data an app shares with other organisations by going to its page in the Google Play store and clicking on "Data Safety." The more data, and the more companies with access to the data, the more potential for exposure and risk is involved with survivor data.

What are the app developer’s data retention and deletion policies?

The practicalities of a co-parenting/visitation app, especially one ordered by courts, may require that data be retained for a certain amount of time. However, this does not mean that all of it should be retained indefinitely. Does the app allow users to delete their data if the case is resolved and the app is no longer necessary for their, or the court’s purposes? What data does it store (and how is it protected)? For how long? Keeping data when it is no longer needed, or using poor cybersecurity practices in storing it, creates a risk if the app developer is ever hacked.

When courts or supervised visitation centers require victims to use specific apps, it’s crucial to consider the potential safety risks and support survivors by incorporating safety planning. Collaboration with local domestic or family violence (DVF) programs or state coalitions can provide valuable expertise and resources. By working together, we can create a comprehensive approach to addressing tech safety, ensuring survivors are informed and supported in their use of required technology. Since most judges, officers of the court, and supervised visitation providers are not experts on cybersecurity, it could also be helpful to work with an outside consultant. An IT professional with expertise in cybersecurity or data privacy may be able to assess whether an app has adequate security in place.

Acknowledgement

This handout has been created by Wesnet under licence from the National Network to End Domestic Violence.