Safety in a Mobile World:
A Look at "Apps"

Our lives have gone mobile. Personal use of smartphones and tablets is rapidly increasing and people are carrying a computer in the palm of their hands. For survivors of domestic or sexual violence or stalking, their mobile phone may be a critical component to their safety and privacy planning. Additionally, mobile phones can also play a role in violence prevention.

Given the prevalence of phones and tablets, it is important to address apps –software applications that run on mobile devices. Billions of apps have been downloaded on smartphones and tablets and hundreds of apps are developed each day. Developers have tapped into every conceivable user's need, including personal safety, awareness building, and violence prevention. But are those apps designed in ways that reinforce concepts of personal safety as we in the violence prevention movement articulate them? With so many apps available, how do we choose the right one for our safety needs?

What makes an app safe?

Survivors / Advocates should look for:

- **Source** – Who manufactured the app, and where does the content come from? The app's content source is important because these apps address the complex topics of domestic violence, sexual assault, and dating abuse and should be developed by or in collaboration with organizations with expertise in these areas. If developed by a company that does not have this expertise, it is likely that the app may contain information and suggestions that are not actually considered safe or recommended by experts.

  Survivors should always know that the abuse is not their fault and that abusers should be held accountable for their behavior. Apps that help survivors regain control, collect evidence, quickly contact help, or provide general information can be helpful; however, apps cannot control someone else's behaviors and, by themselves, prevent abuse.

- **Access to Accurate Information** – Survivors and their advocates are often seeking educational information and helpful resources, possibly in a crisis situation. Does the app contain relevant and accurate information or is their listing of resources out of date?

- **Safety Planning Assistance** – Different apps offer varying versions of safety plans. It's important that survivors get information that is helpful and applicable to them. If the app is specifically designed for college-aged students and discusses safety planning in dorms, that might not be as applicable to an older adult who is relocating to another state. Look for apps that meet the needs of the individual survivors.

- **Privacy** – Does using the app enhance or compromise safety? A well designed app addressing abuse and safety will have explicit and robust privacy woven into the entire design of the app and is clearly explained in the app store. These privacy features should be easily accessible. Apps should also have data collection and information sharing policies that take into account survivor's safety, privacy, and autonomy.

Safety in a Mobile World: A Look at "Apps"

Safety Considerations

Abusers and perpetrators often misuse technology to locate, stalk, harass, monitor, scare, and control victims. The last thing we want to do is download an app that claims to help keep the user safe and/or give guidance to a victim and have that app actually have the opposite effect and be a safety risk instead. The following are some things that we should take into account when exploring app options.

Data Collection

Every app on a smartphone or tablet creates and collects data on the device. Just as with a computer, when you use the app, the settings, information, progress, etc. may be saved to local memory so that the app will "remember where you left off" if you switch to another app in your phone and then re-open the app at a later point.

Some apps attempt to address user privacy and possible abuser access to the phone with features that only allow one use per download or minimize information retained. These are details that should be looked at when considering any app. This information may be provided on the app store, some information in the privacy policies on the app's website, and some information not obvious until after download. Of course, regardless of their privacy and safety features, an abuser could still find an app on a phone if it is not fully deleted by the user. Ideally, apps targeting survivors of abuse should have upfront safety warnings about the possibility of the abuser finding the app on the phone.

Additionally, many apps ask the user for information without any disclosure of where that data is stored or how it may be used. Age or zip code might be requested, for example, to provide usage stats to the developer. This can be very identifying information and survivors who are concerned about their privacy should opt-out. If opt-outs are not available, then another app may be better.

Some apps may request information that isn't relevant to the app's purpose. For example, an app that doesn't need the user's location may still request access to the location information. Few apps allow the user to choose if they want to share additional information, while most often require that information. If the information is not needed for a feature on the app to function, then users should consider other options or another app. Survivors should only share information that they are comfortable sharing.

Privacy policies should outline what happens to personally identifying information that is collected about the user. Ideally, any information that is collected should not be shared by the company. If information is shared at all, it should only be to comply with state and federal laws. Many privacy policies state that they will share information when they receive a subpoena. Subpoenas can be sent by an abuser's attorney though and almost always are not from a court ordering the information. Anything short of a legal mandate to share information should be directed to the user, giving the user full control over their information. If a company must share information, they should inform the user of the requests.

Safety in a Mobile World: A Look at "Apps"

Safety Check List

When considering apps to recommend or discussing a survivor's mobile device usage, here are some questions to help guide those conversations:

- Does the app allow for password protection so only the user can open the app and not anyone with access to the phone?
- Does the app describe personal safety in the context of abuse perpetrated by an intimate partner?
- Does it provide warnings to the user about the app being found by the abuser? Are these warnings provided before the app is downloaded or after the app is activated on a mobile device?
- Does the app have a privacy policy? This should be either within the app itself or on its website. If a privacy policy is unavailable, consider using another app, particularly if the app requests any personally identifying information from the user.
- Does the app require an email address or other contact information in order to use it? Does it ask for other types of personal information (such as the user's or the abuser's physical description, for example)? Is there a disclaimer explaining how data is stored or used?
- Does the app require that a phone or tablet's location services be active in order for the app to work or be useful? Can you refuse the app access to the device's location services?
- Does the app provide inaccurate information or recommend actions that go against suggested best-practices when working with victims (such as suggesting the user inform the assailant that they are being recorded)?