Should I Use This Documentation App?

This post is part of a series on Documenting During Internet Shutdowns. A comparison chart of various documentation apps is available ~~here~~ forthcoming.

Last reviewed: 31 January 2020

There are many apps that documenters can use to capture video, ranging from your phone's native camera app, to more specialized documentation apps like ProofMode, Tella, or Eyewitness to Atrocities. Some apps have features that rely on internet access, so keep in mind that those features may not be available in the event of an internet shutdown.

We can't tell you which specific app is the most appropriate for you, since that depends on your situation, needs, and risks (check out this blog post for more on how to assess your risks and threats). With your risk assessment in hand, these guiding questions below can help you evaluate which video documentation app might work best for you.

Who made the app and do I trust them?

You should always consider the creators of any app that you download and install on your device, and whether you can trust them to not put you at risk, intentionally or unintentionally.

Some things to look out for are:

- Is the app developer reputable? What are people in your community and wider network saying about them and their tools?
- Is the app developer vulnerable? Consider their context and how likely they could be compelled to hand over your data or create a backdoor for authorities (or whether they've actually done so in the past). What country is the data stored in and what are the laws concerning court orders in that jurisdiction?
- Is the app developer maintaining the app? Unmaintained tools are susceptible to hacks that exploit discovered vulnerabilities. Check the developer's website or the app's Google Play page for the "last updated" date.
- How established is the app developer, and does it seem like they will be able to sustain the app over time?
- Is the app open-source? Apps that are open to scrutiny are more likely to have their security issues addressed or at least identified. Is the developer being transparent about the efficacy and security of the app?
- What motivations or incentives drive the app developer's work, and how might that influence their trustworthiness? For example, are they mission-driven? For-profit? Sponsored by a particular funder?

- While not a direct indicator of trustworthiness or not, the cost of the app may be an important consideration. Some apps have a high monthly subscription fee or per-video fee.

Check out the EFF surveillance self-defence guide on choosing apps for more.

Where is the app downloadable from?

You should always only download and install apps from reputable app stores or websites. Even if you have done thorough research to determine the trustworthiness of an app, sketchy app stores may misrepresent their wares and lead you to download an illegitimate imposter created for nefarious purposes. For example, last year the digital rights organization SMEX issued a warning about various websites marketing an app called “WhatsApp Plus” (to be clear, this is not a WhatsApp product!), which could potentially be saving and selling users’ data, or enabling phones that install it to be hacked.

Some security-conscious developers even provide cryptographic keys that enable you to verify their authenticity. They will usually provide an explanation for how to verify these signatures.

Where will the data be stored?

Some documentation apps only store your data and documentation locally on your device, while some only or additionally send and store your data elsewhere. In many cases this is inherent to the design and purpose of the app, such as the Eyewitness to Atrocities app, which sends an unaltered copy of your documentation to a Lexis Nexis storage facility so that Eyewitness can vouch for the chain of custody and integrity of the material. You can only export your media out of the encrypted gallery within the Eyewitness app *after* it’s been sent for safeguarding.

It’s up to you to determine whether you need your documentation to stay on your device only, whether you need it sent and stored to a remote location that you control (as is an option with Tella), or whether to need to send it an external organization / platform that you allow to access and use your documentation. Keep in mind that during an internet shutdown, you won’t be able to transmit your documentation over the internet right away, so you will need an app that at least temporarily enables you store (and ideally back up) your documentation locally (Check out Backing up phone media without internet or a computer).

If your data will be sent to a remote location, be aware of which countries the data will reside. How vulnerable is data to being exposed in those countries, whether by court orders or other means? What risks do you face by having your data exposed there?

Does the app encrypt my media?

Some apps, such as Tella and Eyewitness to Atrocities, provide file encryption and/or encrypted storage for your documentation, separate from your phone’s main gallery and your phone’s encryption, so that your media and metadata are never unencrypted on your device unless accessed through the app with a passcode. This means that even if your phone is unlocked, your documentation remains encrypted. This can provide an extra level of protection for your documentation.

If the app sends and stores your media to a remote location after your internet is restored, also consider whether you need your media to be encrypted while in transit and while in the remote location, as the EyeWitness app, for example, does.

Keep in mind that while encryption is legal in most places, some countries may have laws that restrict or criminalize its use. This map (comprehensive, but from 2017) provides a good starting place if you have questions about the laws in your country.

Does the app capture important metadata (without internet)?

Metadata is data that describes your video or photo, like the time and date or the location. This information is valuable for identifying, understanding, authenticating, and verifying your video or photo as documentation of a specific event. In the context of an internet shutdown, an app's ability to automatically collect certain metadata and/or to allow you to easily input useful descriptive information on the spot is especially useful, as there may be a long period of time before you can share the documentation with anyone (time during which details can be forgotten, circumstances might change, etc, etc).

Most specialized documentation apps such as ProofMode have enhanced metadata features, and gather more metadata than typical built-in camera apps. Enhanced metadata might include various sensor data, nearby wifi or bluetooth signals, device data, cryptographic hash, and user-supplied information, all which can facilitate authentication and verification of the media later on.

Keep in mind that during an internet shutdown, you will need an app that does not require data to be transmitted in order to generate or record the metadata. Some apps may rely on the internet, instead of the hardware sensors, to collect certain metadata. For example, if the location data is captured from look ups on the device, the metadata may reflect the last location where the device had data connection, instead of the actual position of the hardware. The app should also ideally allow you to store the metadata locally without internet, including saving any forms you are filling out (e.g. Tella's "offline mode").

Can I export data from the app?

Depending on your intentions for the documentation, it may be essential to be able to export the video documentation and its metadata from the app, in a format that is not proprietary to the app; that is, to be able to open, view, and use the media and metadata outside of the app. The ability to export means that you and others are not dependent on a single app or service provider to access your documentation, and gives you more leeway in working with the content going forward. Keep in mind that some metadata may not be comprehensible if you do not have access to certain databases or conversion charts to interpret the numbers (for instance, in the case of cell tower IDs or Wi-Fi networks).

Note that some apps may have a deliberate closed chain of custody and not allow users to export, while some apps may simply not be designed with an export use case in mind. Also be aware that some apps, like Eyewitness to Atrocities, may not let you export until you have uploaded the media to a remote server (which you need internet access to do), and some apps may allow you to export the media, but not the metadata (other than any metadata that lives in the file itself).

If you need to export, ideally your app should allow you to export a copy of the media without any changes or transformations, and a copy of the metadata in a standardized readable text format. Tella metadata, for example, is stored encrypted in the Tella gallery, but can be exported as CSV. Additionally, during an internet shutdown, it is necessary to have options for exporting to offline apps or non-internet dependent services. Most apps that allow you to export have some kind of “Share” button that triggers a share menu, which Android populates with a list of apps on your phone that are capable of handling that type of content. Unfortunately app developers can customize their share menus and there is no consistency between apps.

For a larger quantity of files, it may be more efficient to access the stored files via a file manager app and copy the files from there, although you may not be able to access metadata stored in an app’s database this way. This option is also not available for apps that provide their own secure galleries, as the files will be encrypted in storage. For these apps, it is necessary to have a sharing function within the app.

Check out our comparison chart of documentation apps, and the next post in this series, “Maintaining Verifiable Media During an Internet Shutdown.”