VIDEO AS EVIDENCE: TECH TOOLS
FOR TRANSFERRING FILES

Filming for human rights can be dangerous. It can put you, the people you are filming and the communities you are filming in at risk. Carefully assess these risks before you press "record".

Do your best to implement the guidance below, but understand that nothing stated in this guide is absolute. You should modify the practices to fit your needs. When possible, seek support from local experts. Even if you cannot fully implement this guidance, your footage may still provide valuable information that could lead human rights organizations and advocates to answers and, in turn, to the protection of our basic human rights.

INTRODUCTION

Tools for File Transfer

In any situation where video is collected for use as evidence there will come a time when the footage needs to move from the custody of those capturing events to the custody of those who will store and use it. Transferring files often has to happen in the field under less than ideal conditions, so doing so safely and reliably can be difficult.

The process of organizing this footage for transfer may involve gathering video from many different people; it may encompass a range of devices, from phones to cameras to computers and hard drives; and in some circumstances there will be a need to guard identities of those involved or the content itself from potential adversaries. For all of these reasons, it is important to think through both the workflow of how video will be collected and transferred from the field, as well as the tools that will be used to make it happen.

STEP 1 What Are Your Needs?

As with any task, you must assess your needs before choosing the right tools for the job. Here are four factors to think through at the outset:

- **WORKFLOWS:** Are you moving files to or from one or many sources? Are you transferring files to or from people you partner with closely, or are you working in a more open process? Do the videos and other files need to be available online for multiple users at once? How tech savvy are your partners, and what tools are they already familiar with?
- **SECURITY:** Do you need to keep the content of media files away from prying eyes? Do you need to maintain personal anonymity on one or both sides of the transfer? Do you need to protect the anonymity of individuals who appear in the video?
- **CONNECTIVITY:** Does everyone you're working with have reliable access to strong Internet or mobile networks? Is there a need to access anonymous or encrypted channels, and, if so, is everyone in your workflow aware of how to do so? Does the transferring need to happen in the field or can you take it back to your home or office?
- **FILE SIZE:** Are the files being transferred short videos shot on cellphones, or are they longer videos coming from high-quality cameras? Are you transferring one or a few pieces of media from each source, or are you moving a large stockpile of media from one place to another?

KEY DECISION POINT

Online Or Offline Transfer?

Despite the fact that many of us are constantly connected online, it is often the case that transferring files offline is the best choice. Documenters in some locales will be dealing with poor Internet connectivity, and if it is necessary to use encrypted and/or anonymous channels, the already time-consuming process of moving big files can slow to a crawl, even if you are not burdened by low bandwidth. The complexity of keeping video files anonymous and encrypted may mean that documenters and their partners feel safer physically handing over files. In these cases, it makes more sense to use offline storage like flash drives, external hard drives, and SD cards, in combination with encryption and good operational security, to move files from one place to another.

STEP 2 Determine Which Type Of Tool Works For You

Once you answer those basic questions about the process, risks, and players involved, you can narrow down the options for moving files. Broadly speaking there are three categories of file transfer tools, and each one addresses different needs.

A: ONLINE SHARING: Online or "Cloud" storage has rapidly grown in popularity as a way to provide others with access to your media files, becoming easy to use and widely available with tools like Google Drive and Dropbox. But there are potential pitfalls - managing access to files, staying under restrictive storage limits, and, most importantly, keeping your videos private and secure. Most popular services do not adequately encrypt your files, and when these services do have encryption they often hold the keys, so they can access your files and could turn them over to any authorities who come asking. To make sharing in the cloud more secure, try using add-on tools, switching to "zero-knowledge" cloud storage providers that are built for privacy, or setting-up a secure server where files can be securely and anonymously uploaded.

- **BOXCRYPTOR:** An add-on tool that provides full encryption for those using cloud storage like Dropbox or Google Drive, Boxcryptor uses public and private keys to encrypt files for sharing with particular users.
- **SPIDEROAK:** A leading encrypted cloud storage option, SpiderOak allows transferring via password-controlled "Share Rooms" that can be linked to other users, even if they don't have the application downloaded. Similar options include Wuala and Viivo.
- **SECUREDROP**: An open source platform for setting up a secure file transfer server, SecureDrop has been adopted by media outlets looking to provide a safe space for whistleblowers to share files. GlobaLeaks is another opensource option.

KEY DECISION POINT

Sharing On Social Media

Files are often shared on social media and commercial content platforms but this is far from ideal. Potential issues include a loss of privacy, the loss of important metadata in the original video files, and the removal of the video by the platform if the content is considered too sensitive among others reasons.

B: DIRECT DIGITAL SHARING: Directly transferring big files from one person to another has always been difficult on the web, and unless you have web hosting or can run your own server, it's still a challenge. The most common way to send a file directly to someone is email, but when it comes to video, that method can be extremely slow, limited to files of a certain size, and insecure. Often documenters in the field shooting mobile video will use messaging apps like WhatsApp to share their files, but those methods are less than ideal for many of the same reasons as email. For those working together in the same vicinity, Bluetooth, WiFi Direct, and other near-field communication (NFC) technologies are all secure and simple options, but work best if you are only moving a limited number of smaller files.

- **BLUETOOTH:** The same thing that connects your wireless keyboard or mouse to your computer, Bluetooth is a secure option available on even the simplest feature phones, but its slow transfer speeds make it an impractical option for transferring more than a few files.

- **WIFI DIRECT:** An updated protocol with speeds up to ten times faster than Bluetooth, WiFi Direct is available on newer smartphones. NFC-equipped devices use WiFi Direct to tether to other devices and transfer files.

- **BITTORRENT SYNC:** BitTorrent Sync is a file transfer application based on the BitTorrent protocol, and it allows a range of private and encrypted sharing options. Be aware, though, that it is not open source, which means its code cannot be publicly audited for security flaws, and it requires that each device be powered on at the same time for the file to transfer.

C: PHYSICAL STORAGE: It often turns out that handing off or mailing an SD card, flash drive, or hard drive is the safest and simplest way to transfer files. Poor connectivity, limited technical knowledge among partners involved in a transfer, or security concerns may push you towards the tried and true option of transferring files offline.

- **EXTERNAL HARD DRIVES:** External hard drives can hold terabytes of data, while flash drives are small enough to fit discreetly in your pocket but come with limited capacity that can run out quickly if you are moving videos. One good option is the Seagate Wireless Plus which has 1 terabyte (that's 1000 gigabytes) of storage, is battery-powered so it can be used to backup and transfer files in the field, and is WiFi enabled. Similar options include the Kingston Wi-Drive.

- **MicroSD CARDS:** As for smartphone storage, many come with microSD cards that can easily be swapped out and passed to others, though they are becoming less common due to the constant demand for thinner and sleeker phones. Compatible with some Windows and Android phones, GoPros and a range of cameras, these cards offer a cheap option for getting a lot of storage, up to 128GB, that can be easily shared given their tiny size.

- **USB TRANSFER:** Transferring from smartphones or other devices to a computer or external hard drive can obviously be done with the standard USB cables, as well, but if all you have is a phone and a flash drive, you will need an extra cord to make them compatible. The USB On-The-Go (or USB OTG) can be purchased inexpensively online and provides a way to connect a flash drive directly to a smartphone.

TECH TOOLS UPDATES

Tech tools are always changing! Visit the WITNESS blog for the latest information and reviews: blog.witness.org

STEP 3 Double Check Your Security

Security should always be a priority when dealing with evidentiary video. Be sure to include encryption and anonymity in your workflow (and make sure you know the difference between the two). Encryption is an important step no matter which transfer method you opt for, and it can be done in a couple of ways.

Option 1: Full Disk Encryption

Create encrypted volumes on your computer or external storage device. Your operating system comes with built-in tools that allow you to do that, though they are not very convenient if you need your encrypted drives to be usable on devices with different operating systems (for example, when moving from a Windows computer to a Mac). If that's the case, look to a third-party application that can work across PC, Mac, Linux, Android and iOS; just be sure to check the latest security updates to make sure they are still considered safe and, in the case of an open source option, have been audited recently.

- **SUGGESTIONS:** FileVault on Mac OSX and BitLocker on Windows are the built-in options; TrueCrypt, VeraCrypt, and Symantec Endpoint are cross-platform applications. HFSExplorer is an example of a tool that can open a Mac-encrypted DMG volume on Windows. On mobile, Android devices have an encryption option in the settings, though it will slow the device down and there is no easy way, short of a reset, to turn off the encryption.

Option 2: File Encryption

Directly encrypt individual files, rather than whole drives. The best way to go about this is to use the PGP standard, which you may already be using to encrypt your email. This method is very secure and well known, but it requires everyone involved in the transfer to have PGP keys set up and made available to each other, so a bit of preparation is needed.

- **TS:** GPGTools for Mac, Gpg4win for Windows, and Android Privacy Guard (APG) for Android-based smartphones are the best options for using PGP to encrypt your files and share them with specific people.

KEY POINT

Protecting Anonymity

The full disk encryption and file encryption approaches protect the content that you're transferring, but if you need to keep yourself anonymous online when setting up accounts and navigating the web, the Tor Browser is a good place to start. A VPN service is another option that may provide a bit more cover depending on where you are, though VPNs should be avoided if using the torrent option mentioned above. If complete anonymity is needed – when using a public computer, for example -- the TAILS operating system can give you access to browsers and basic applications while not logging any of your activity on the hard drive.

LEARN MORE

The landscape of technologies is constantly changing, and researchers and activists are constantly finding new methods - and threats - when it comes to digital security. Check out **Tactical Tech's Security in a Box** (https://securityinabox.org/en) or the **Electronic Frontier Foundation's Surveillance Defense tools** (https://ssd.eff.org/en) for additional information about protecting your digital security.

The resources suggested in this document are focused on getting files from one person to another, but managing them once they reach their destination is a complex and important task in its own right. Here are a few suggested resources on media management:

LIST OF RESOURCES

- **The Video as Evidence Field Guide** (http://bit.ly/WITNESSLibrary_VaE)
- **The Activists' Guide to Archiving Video** (http://archiveguide.witness.org/)
- **WITNESS Library** (library.witness.org)

Stay updated on new tools and how activists are using them around the world on the **WITNESS blog** (http://blog.witness.org/).