A WITNESS TIP SHEET

TRANSFERRING HUMAN RIGHTS VIDEO ONLINE

FILMING FOR HUMAN RIGHTS CAN BE DANGEROUS: BE SAFE. BE ETHICAL. BE EFFECTIVE.

Using human rights video requires handling the videos carefully throughout their lifecycle, especially when the video is being electronically transferred from one place to another. This chart provides a comparison of popular services/systems and important factors to consider for best protecting the authenticity, integrity and usability of your footage. Always research the most current terms of service before making a decision.

KEY FACTORS	YOUTUBE	DROPBOX	SKYPE	GMAIL/GOOGLE DRIVE	INTERNET ARCHIVE
Permanence: The system/service will not remove or delete your videos without your authorization, or provides adequate advance notice. Useful when you cannot download immediately after upload.	YouTube can remove videos at any time without notice, especially if the content is graphic. YouTube weighs the amount and quality of information in the title and description when deciding whether or not to remove an item, so always include basic information about your video.	Dropbox generally will not remove your files, but can terminate any account with advance notice. It is possible to restore accidentally deleted files for 30 days (or longer with Packrat feature).	No permanence. Skype only transfers files; it does not store them.	Google generally will not remove your files, but can terminate accounts. Files that are deleted by the owner cannot be recovered.	Internet Archive will not remove your files unless they receive a valid request from a rightsholder. It can terminate accounts at any time, upon written notice.
Data Integrity: The system/service enables you to download an exact copy of what you uploaded, without alteration, data loss or corruption.	Uploaded video files are not retained in their original format. Only a transcoded copy can be downloaded.	Files can be transferred and downloaded intact. You can also restore deleted files.	Files can be transferred and downloaded intact.	Files can be transferred and downloaded intact.	Files can be transferred and downloaded intact. Hashes/ checksums are computed and saved in an accessible text file.

KEY FACTORS	YOUTUBE	DROPBOX	SKYPE	GMAIL/GOOGLE DRIVE	INTERNET ARCHIVE
Privacy: The system/ service is not vulnerable to unauthorized access. If you have confidential information, the system allows you to encrypt or limit access to select files.	YouTube is designed for viewing access, but there are options for setting "private," "unlisted," and "public" videos.	Dropbox Transfer uses SSL, and files are encrypted on server. Encrypted files can be uploaded. Owner controls sharing for each file, but there is no read-only option. There is a 2-step verification option. Desktop and mobile application may compromised if computer is taken/attacked.	Skype encrypts its network traffic, including file transfers. Encrypted files can also be sent. In some cases, real-time transfer can be more secure than keeping files on a remote server, although the locally stored files and Skype history may be a security problem if computer is taken/attacked.	Google transfer uses HTTPS/TLS. Google does not encrypt files on server, but encrypted files can be uploaded. Owner can control read/ write/ download access to files. There is a 2-step verification option. Desktop application may be security problem if computer is taken/ attacked.	Anything uploaded can be viewed, accessed, and downloaded by anyone.Encrypted files can be uploaded, but anyone can access and download them.
Chain of Custody: The system/service monitors and logs activities that affect the video (e.g. who uploaded and when, who accessed and when, who edited and when, etc), and allows you to access this information.	Accessible data includes date uploaded, date published, date updated, YouTube user ID.	Account owner can access Dropbox Events, which keeps track of actions related to files, who did them, and when.	Transfer is recorded in Skype conversation history. The log (.DB file) is stored on user's computer.	Revision History shows when a file was uploaded or updated and by whom.	Accessible data includes date added, uploader, dates updated, checksums for all files.
Documentation: If you have metadata that is separate from your video, the system/service allows you to keep this metadata associated with the video.	Uploader can add metadata in title, description, and tag fields. Some metadata embedded in original file is lost.	Documentation can be uploaded like any other file.	Documentation files can be transferred, or entered as part of the Skype conversation and saved.	Documentation can be uploaded as a separate file, or can be created in Google Docs or a Gmail message.	Documentation can be uploaded with the video.
Accessibility: The system/service enables you to access and download your videos on demand.	Downloading copies of videos that are not your own or that do not have a YouTube download link violates YouTube Terms of Service.	Files can be downloaded and shared at any time.	Skype does not store files, so they cannot be accessed later. Recipient must save file locally at time of transfer.	Files can be downloaded at any time. Google Takeout facilitates batch downloads (www.google.com/settings/takeout).	Files can be downloaded at any time.

KEY FACTORS	YOUTUBE	DROPBOX	SKYPE	GMAIL/GOOGLE DRIVE	INTERNET ARCHIVE
Efficiency: The system/service's method for uploading and downloading files is quick and efficient.	Uploader is able to resume interrupted uploads.	With desktop app, folders can be synced across multiple devices.	Potentially slow transfer depending on connection. Interrupted transfers can be resumed, but both parties have to be online at the same time.	With desktop app, folders can be synced across multiple devices. Users can add files to Google Drive directly from Gmail.	Uploader is able to resume interrupted uploads.
Cost: You can afford the system/service's cost to upload and download videos in the volume and frequency that you need.	Free.	No cost for access. Free accounts come with limited storage. Paid subscriptions come with more storage.	Free.	No cost for access. Free accounts come with limited storage. Paid storage plans provide additional storage.	Free.

FILE TRANSFER PROTOCOL:

FTP is a network protocol for transferring files between two points over the Internet. Users can upload and download files from an FTP server (your own or a hosted service) using an FTP client application. However, FTP lacks security, putting the information shared at risk if the file transfer is intercepted.

Permanence: FTP is just a way of transferring files, so permanence depends on who is hosting your FTP server.

Data Integrity: Files can be transferred intact.

Security: FTP is generally unencrypted and not secure, but you can FTP encrypted files.

Chain of Custody: Depending on the software, users may be able to create log of transfers.

Documentation: Documentation files can be transferred with video files.

Accessibility: Files can be downloaded at any time, depending on your FTP server.

Efficiency: FTP is able to resume interrupted uploads.

Cost: No-cost FTP software is available, but there may be costs associated with running or using a server to host and provide the files.