Metadata

How to ensure you don't accidentally send private information along with your photos.

RhED

1800 458 752
sexworker@sexworker.org.au

When taking a photo on your smart phone or digital camera, metadata is stored alongside each image. This can include information such as;

- the date the photo was taken,
- the make and model of the device the photo was captured on,
- the GPS coordinates of where the photo was taken.

Metadata is automatically stored in Exif (exchangeable image file format) by the phone or camera that digitally captured the image and is typically embedded internally in image file formats such as PNG and JPEG.

Many social media and messaging sites used by sex workers such as Twitter, Instagram, Facebook, and Whatsapp strip Exif data before the images are visible to other users. If you have your own website with uploaded images, it may be possible to find metadata in these attached photos. Depending on how the website is set up, popular website builders (such as Squarespace) do not automatically remove all metadata from uploaded images. For example, if your Squarespace website allows for images to be downloaded by users, metadata will typically remain embedded unless you (or your photographer) have removed it prior. Similarly, if you send a photo you have taken on your device via email or SMS, the Exif data will typically go along with it unless you have removed it prior.

Removing Metadata

The steps to remove Exif data can vary depending on your device.

Location data

Removing location data is probably the highest concern for the sex work community. Firstly, if you're capturing (and sharing) images on a smart phone be sure to turn off your location settings so location data is not captured alongside your images.

iPhone: To turn location settings off,
- Go to 'Settings,'
- Tap 'Privacy,'
- Select 'Location Services,'
- Tap 'Camera,'
- Select 'Never.'

Android: To turn location settings off,
- Go to 'Settings,'
- Tap 'Privacy,'
- Select 'Permissions,'
- Tap 'Location,'
- Open 'Camera,'
- Select 'Deny.'

BHN
Better Health Network

Metadata

How to ensure you don't accidentally send private information along with your photos.

RhED
1800 458 752
sexworker@sexworker.org.au

To remove Exif data on your device after an image has been taken, there are free apps on both iPhone or Android. Another (simpler) way to do this is to take a screenshot of the photo and share the screenshot instead. Screenshots don't typically include the same type of sensitive metadata as a camera captured image.

Also note, the use of some photo editing apps may further add metadata onto your images which can include timestamps, systems information, and any tracked changes to the image.

Laptop and desktop computers

You can remove or check for Exif data on photos already captured using your laptop or desktop.

Windows: Right click on your photo to see if there is Exif data attached,
- Select 'Properties,'
- Check under the 'Details' tab; here you can also remove most Exif data (including location).
- Click 'Remove Properties and Personal Information', then save the file.

Mac: Open the image in 'Preview,'
- Go to the 'Tools' menu,
- Select 'Show Inspector,'
- If your image contains Exif data, there will be a tab labelled 'Exif'.
- There will also be a 'Remove Location Information' button that will delete location data.

Further Reading

A general overview of metadata

What can metadata tell you

Steps on removing or checking for Exif

Squarespace and metadata

BHN
Better Health Network