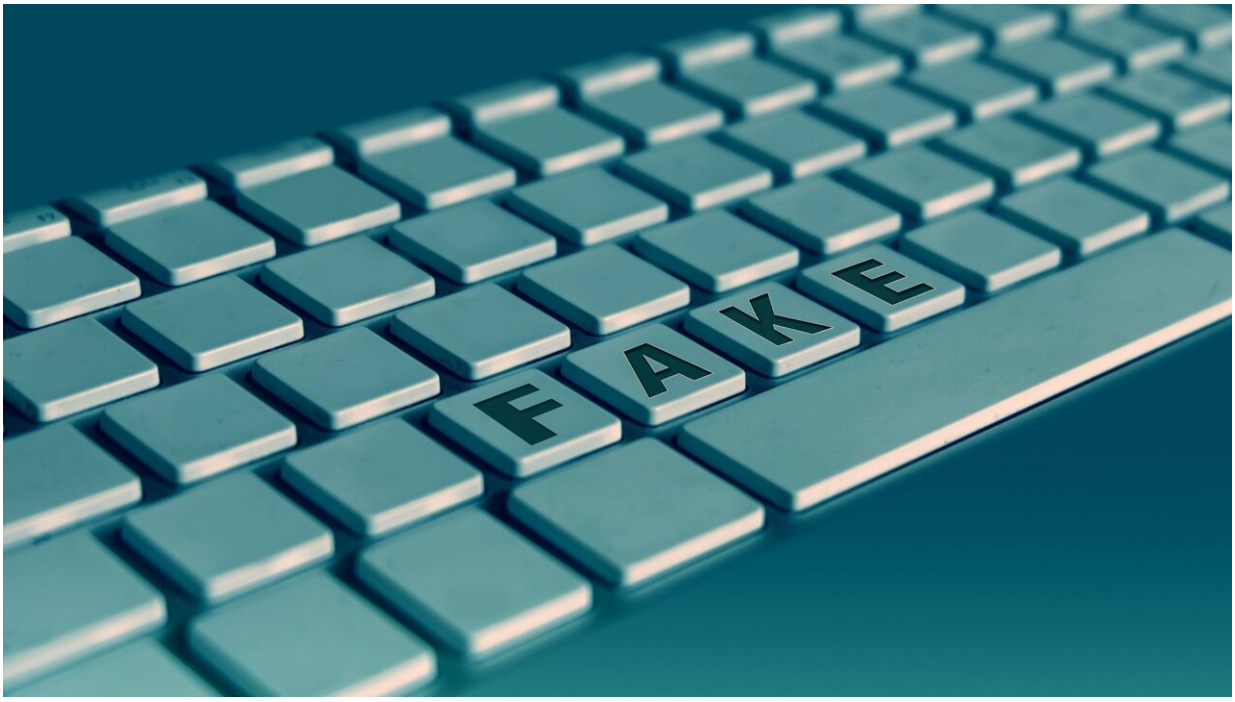
Open-source imagery is transforming investigations of international crimes—but how do judges know if it's real?

September 11 2024, by Sarah Zarmsky, Alexa Koenig and Yvonne McDermott



Credit: Pixabay/CC0 Public Domain

Open-source online imagery can play a vital role in investigating and prosecuting alleged crimes—but only if courts can reliably assess its authenticity.

Unfortunately, what we see online can't always be trusted. Misinformation and disinformation are rife on social media, and advances in technology have made it easier than ever to manipulate or fabricate images—even generating them entirely through algorithms.

To help legal professionals navigate these challenges, we and our colleagues have created a guide for judges and fact-finders to better assess digital open-source content. This guide explains important terms and techniques for evaluating the reliability of online information, ensuring it can be used effectively in legal proceedings.

For evidence in international courts and fact-finding missions to be useful, it must be relevant, authentic and reliable. This is critical not only for ensuring justice for the accused, but also for establishing an accurate historical record.

The photos and videos you may have stumbled across on social media are examples of digital open-source information. This is publicly available data that can be accessed online at little or no cost.

In international law, this type of information is increasingly being used as evidence in courts and by human rights bodies. But it presents unique challenges in terms of reliability and authenticity.

Unreliable content

There are many reasons that a piece of content may be unreliable. For example, content may be misattributed or decontextualized, as in the case of a video that allegedly depicted Turkish attacks in northern Syria in 2019. Having circulated in mainstream news, it was eventually found to be footage from a gun range in Kentucky, US.

It is also possible for content to be staged and falsely attributed to real

events. A well-known example of this was the "Syrian hero boy" case in 2014. A video allegedly depicting a boy saving a young girl from gunfire during the Syrian conflict was later proved to have been staged and shot on a film set in Malta.

Content may also be manipulated or generated using artificial intelligence (AI). An example of this emerged in 2022 in the context of the war in Ukraine. A purported video of President Volodymyr Zelensky telling his soldiers to lay down their arms and surrender to Russia was ultimately debunked and removed from social media platforms.

A content's metadata, its "data about the data," may suggest how, when and by whom a digital file was collected, created, accessed, modified or formatted. Metadata can help reveal if an image is a deepfake, or if the time, date or location of capture do not match those of the relevant event.

But metadata can also be manipulated or deleted, so it should always be viewed as part of an overall analysis of the content.

How to verify online imagery

One of the most critical indicators of a video or photo's authenticity and reliability is the source. Evaluators should assess whether the source is known. If so, they should ascertain whether the source may be subject to potentially problematic biases, or has a track record of posting unreliable content.

If a source is unknown, extra care should be taken to assess the content's authenticity and reliability. For example, the source of a video depicting the killing of two women and two children in Cameroon in 2018, which was shared widely across the media, was anonymous. Researchers from BBC Africa Eye were able to use other information from the video to

assess its authenticity. It ultimately aided in the investigation and conviction of the perpetrators.

There are also multiple methods that anyone can use to confirm where a piece of content was captured. For example, reverse image searching is a process by which a person can use a search engine to see whether the image or a similar one has appeared online previously.

Matching geographic features in an image to satellite imagery is another technique. For example, researchers at the University of Essex matched features in an open-source video to those shown in satellite imagery when investigating the alleged killing of unarmed protesters in Nigeria in 2020. It established that the video did, in fact, depict the claimed location in the country.

When determining when a photo or video was taken, investigators can use contextual clues, such as the weather. For time of day, investigators can use techniques such as shadow analysis, which measures the length of shadows cast by objects and people in a particular location on a particular day, to indicate the position of the sun and therefore the time.

An illustration of this technique appears in a 2014 Bellingcat investigation which tracked the movements of a Buk missile launcher, and ultimately discovered Russia's responsibility for the downing of Malaysian Airlines flight MH17 over Ukraine.

Evaluating whether a piece of open-source imagery is what it's claimed to be relies on multiple methods of analysis. There is no single method or tool that can or should be used on its own. Nor can we rely solely on AI to automatically detect what is real and what is not.

Our guide aims to equip judges, investigators and the public with a deeper understanding of how to analyze and verify online imagery. By

mastering these techniques, we can better uncover the "who, what, when, where, why and how" of digital evidence, strengthening justice for international crimes.

Provided by The Conversation

Citation: Open-source imagery is transforming investigations of international crimes—but how do judges know if it's real? (2024, September 11) retrieved 11 September 2024 from https://phys.org/news/2024-09-source-imagery-international-crimes-real.html