VERIFICATION HANDBOOK

AN ULTIMATE GUIDELINE ON DIGITAL AGE SOURCING FOR EMERGENCY COVERAGE.

EDITED BY CRAIG SILVERMAN
EDITOR OF 'REGRET THE ERROR': THE POYNTER INSTITUTE
One powerful image can define a story.

That was certainly the case for BBC News' User Generated Content hub in the beginning of July 2005. It had been one week since the initial pilot team was set up to help collate the content being sent to BBC News by its audiences, and help get the best of it shown across TV, radio and online.

Then the July 7 bombings in London happened.

That morning, as the BBC and other news organizations reported a power surge on the London Underground, the UGC team started seeing a very different story emerging via content sent to BBC News directly from its audience.

Photo: Alexander Chadwick

This was one of the first images the team received. Before it was broadcast, the image was examined closely and the originator was contacted to verify his story and the details of what
he saw. The photo inadvertently became one of the first examples of the UGC image verification process that has since moved toward standard practice across the industry.

That image, and others like it, showed the terror and chaos in London during the moments immediately after the attacks. As a result, it ensured that the reporting of the story quickly changed. It was the first significant example of UGC's proving critical to helping BBC News tell a major story more accurately, better and faster.

Today, the UGC team is embedded within the heart of the BBC newsroom. Its 20 journalists work across TV, radio, online and social media platforms to produce content sourced either directly from the BBC’s audiences or from the wider Web.

Verification is critical to the success of what the UGC team produces. Technology has moved on considerably since 2005, bringing an exponential rise in the use of social networks and the power of mobile phones. These changes offer great benefits in our newsgathering processes, particularly on breaking news; they also bring great challenges.

Whether a trusted global news organization like the BBC or a humanitarian professional on the ground, the need to be fast at collecting and disseminating key images on a breaking news story has to be balanced with the need to be sure the images are credible and genuine. We also have to ensure copyright is protected and appropriate permissions are sought.

Since that day in 2005, the UGC team has developed a number of approaches to help in this process. While the technology will continue to change - as will the tools we use - the basic principles of image verification remain the same:

1. Establish the author/originator of the image.
2. Corroborate the location, date and approximate time the image was taken.
3. Confirm the image is what it is labeled/suggested to be showing.
4. Obtain permission from the author/originator to use the image.

Let's look at these points in more detail.

1. Establish the author/originator of the image

The obvious - and usually most effective - way of doing this is to contact the uploader and ask him directly if he is indeed the person who took the image.

Reaching out to the uploader via the social network account or email address the image was shared from is a first step, but it’s also important to try to ascertain as much about the uploader’s identity as possible. These details can help in determining whether he is in fact the original source of the image.
As outlined in the previous chapter, in many instances, people may try to be helpful by reposting images they have seen elsewhere. This happens frequently to news organizations - images are sent in by well-meaning members of the public to help report a story. Just by asking the sender to confirm if it's his image or not can save a lot of time in the verification process.

While tracking down the source of an image begins with the person who uploaded it, it often ends with a different person – the one who actually captured the image.

As referenced in an earlier chapter, an important step is to use a service like Google Reverse Image Search or TinEye. Paste the image URL or a copy of the image into either and they will scan the web to see if there are any matches. If several links to the same image pop up, click on “view other sizes” to investigate further.

Usually, the image with the highest resolution/size should take you to the original source. (On Google Images, the resolution for each image result is listed just next to the image itself.) You can then check it against the image you have and see if the source appears authentic.

Quite often on a breaking news event, there will be no images of specific people that you want to illustrate the story with (particularly if they involve ordinary members of the public). Alternatively, you might want to confirm that an image you have of someone is actually them and not someone else with the same name.

I've found Pipl.com to be particularly helpful here as it allows you to cross-reference names, usernames, email address and phone numbers against online profiles of people. For international searches, WebMii is an additional resource that can help. LinkedIn is also proving to be a great way of verifying individuals and often provides additional leads for being able to track them down (through companies/organizations they are currently or previously associated with).

2. Corroborate the location, date and approximate time the image was taken

There are some useful journalistic and technical ways of establishing information such as date, location and other important details. One core way of gathering this information is when you speak to the creator/uploader of the image. These five questions continue to stand the test of time:

- Who are they?
- Where are they?
- When did they get there?
- What can they see (and what does their photo show)?
- Why are they there?

One important aspect to note here: If the image is from a dangerous location, always check
that the person you are talking to is safe to speak to you. Also be aware of any issues about identifying the source through any details you broadcast about him or his images.

From our experience at the BBC, people who were really there will give visual answers, often describing the details in the present tense. (“I'm in the middle of X Street; I can see and hear Y.”) The more vague the answer, the more caution you should exercise about what the source is telling you.

Another useful technique is to ask the person to send any additional images shot at the same time. It's rare that someone takes only one picture in a newsworthy situation. Having more than one image helps you learn more about how the events in question unfolded.

Once you've gathered the source's account of how the image was taken, work to corroborate the information further. Two primary methods can be used to investigate the contents of the photo itself and triangulate that with what you were told by the source.

First, check if the image has any metadata. Metadata, also referred to as “EXIF” data when it comes to digital images, refers to information embedded in an image. If the image is an original, there's a good chance you will see information about the make and model of the camera, the timestamp of the image (be careful though - if there is one, it could still be set to the manufacturer's factory setting or another time zone), and the dimensions of the original image, among other details. You can use software like Photoshop (look at the file information) or look for or free online tools like Fotoforensics.com or Findexif.com to generate an EXIF report.

Upload the image and the EXIF reader will return out whatever information is contained on the image. Some of the information is useful to those who have a more technical understanding of digital photography. But for the average person, data such as the date the photo was originally taken or the type of camera that took the image can sometimes help expose a lying source.

One note of caution here: The majority of social media image sites such as Twitter, Facebook and Instagram strip out most of the original metadata from images when they are uploaded onto their platforms, if not all. (Flickr seems to be an exception to this.)

Second, cross-reference the image with other sources. Awaken your inner investigator by examining the image closely. Quite often there will be clues that can help you verify the location and time it was taken:

- License/number plates on vehicles
- Weather conditions
- Landmarks
- Type of clothing
- Signage/lettering
- Is there an identifiable shop or building?
3. Confirm the image is what it is labeled/suggested to be showing

An image may be authentic, but it could be inaccurately labeled. For example, during Hurricane Sandy, this image spread widely on Twitter and was described as being a shot of three soldiers standing guard at the Tomb of the Unknown Soldier during the storm:

![Image of soldiers at the Tomb of the Unknown Soldier](image)

The image was accurate in that it did show soldiers at the Tomb. But it had been taken a month earlier, not during Sandy. The picture had been posted on the Facebook page of the First Army Division East.

As part of verifying the date, time and approximate location of an image, it's also important you confirm that the image is what it purports to be. An authentic image can still be placed
in a false context.

Use Google Maps, Bing Maps or Wikimapia to help you verify locations. UGC images are increasingly being tagged on these services now, and they can also provide useful leads to follow up on, as well as different angles to locations you are investigating. (Learn more about using these mapping services for verification in Chapter 5: Verifying Video.)

Use weather sites that can give you accurate reports of conditions at that location on that date to confirm if the weather in the image matched. As noted in the previous chapter, Wolfram Alpha is very good at searching for weather reports at specific times and places.

If there is lettering (e.g. on a sign) in a different language within the image, use Google Translate to see if it can give you another clue to the location. The optical character reading tool free-ocr.com can also be helpful if you want to extract text from an image -which you can then run through an online translation.

Social media location services like Geofeedia and Banjo can also help establish the location from which an image was uploaded. These services use the GPS data from the mobile device that uploaded the image. While they currently capture only a small percentage of the social media content uploaded from a given location, they do provide a useful initial filter. The image below is an example of some of the photos captured by Geofeedia in the immediate aftermath of the Boston marathon bombings:

![Image of photos captured by Geofeedia](image_url)

Along with those tools and techniques, for images it’s also useful to check to see if similar images are being distributed by official news organizations or agencies. Are there any images from that location being uploaded on social media by others? If they show a similar scene
from a different angle, that will also help establish credibility of the image.

Finally, on a big story, it's always worth double checking if a particularly strong image you come across appears on Snopes\textsuperscript{16}, which specializes in debunking urban legends and misinformation on the Internet.

4. Obtain permission from the author/originator for use of the image

It is always best practice to seek permission from the copyright holder of images. Adding to this, copyright laws in many countries are increasingly clear that damages can be sought by the originator if permission isn't asked for or granted.

The terms and conditions with regards to the copyright of content uploaded on social media sites vary from service to service. Some, like Flickr, show clearly alongside the image if the photographer has retained all copyright, or if he allows Creative Commons usage. (It's a good idea to read up on Creative Commons licenses\textsuperscript{17} so you are familiar with how they differ.)

When seeking permission, it's important to keep a few details in mind:

• Be clear about the image(s) you wish to use.
• Explain how the image(s) will be used.
• Clarify how the photographer wishes to be credited (name, username, etc., keeping in mind that in some cases they may wish to remain anonymous).

Most importantly, remember that if you've gone through the above checks and processes and you're still in doubt - don't use the image!
Case Study 4.1: Verifying a Bizarre Beach Ball During a Storm

Philippa Law and Caroline Bannock lead GuardianWitness, the Guardian’s open journalism platform where readers share their videos, images and stories. Bannock was previously a senior news producer and acting foreign-editor for Channel 4 News. She tweets at @carlanine. Law was a BBC radio producer and has a Ph.D. in audience participation for minority language media. She tweets at @philonski.

Storm force winds and rain brought flooding and power outages to the south of the U.K. in October 2013. This event affected a lot of people, so to widen and enrich the Guardian’s coverage, we asked our readers to share their photos, videos and stories of the disruption via our user-generated content platform, GuardianWitness.

Among the contributions we received was a bizarre photo of what appeared to be a giant multicolored beach ball, at least twice the height of a double decker bus, on the loose at Old
Street roundabout in London. This was one of those images that immediately evokes the question, “Is this too good to be true?” We were very aware that it could be a hoax.

We started verifying the user’s photo by running it through Google reverse image search and TinEye to verify that the image hadn’t been borrowed from another website. Users often try to show us a news event by sending pictures that have been published on other news sites, or shared on Twitter and Facebook. So a reverse image search is always the first check we make.

In the case of the rampant inflatable, Google returned no hits - which suggested the photo was either original or very recent and hadn’t been picked up by any other news organizations - yet. Good content gets published very fast!

The most important verification tool we have is a direct conversation with the user. Every contributor to GuardianWitness has to share an email address, though there’s no guarantee it’s a correct one. So we emailed the user in question to try to make contact. In the meantime we continued with our verification checks.

Usually we would verify where a photo had been taken by comparing it with images on Google Street View, but as our team is familiar with the Old Street area, we recognized the view in the photo and felt reasonably confident the picture had been taken there. Although we knew the area, we didn’t recall seeing a giant beach ball - so we searched online for earlier evidence. We found it had previously been tethered to the top of a building nearby. This finding meant the image was looking less like a hoax than it had first appeared.

We checked Twitter for mentions of the beach ball that morning and were able to confirm that there had been other sightings around the time the user claimed to have taken the photo. Our Twitter search also revealed a later photo, taken by another user, after the ball had deflated.

Finally, the user got in contact with us and, by speaking to him on the phone, we were able to confirm that he had taken the photo himself.

Having taken all these steps to verify the image, we were happy that the story held up to scrutiny. The compelling image of a runaway beach ball in the driving rain was published on the Guardian’s live-blog and was shared widely on social media.
Case Study 4.2:
Verifying Two Suspicious “Street Sharks” During Hurricane Sandy

Tom Phillips is a senior writer at BuzzFeed UK. He previously worked for the UK newspaper Metro, was an international editor at MSN, and most recently helped launch UsVsTh3m, an experimental social-focused “startup” for Trinity Mirror. In his spare time, among other things, he runs Is Twitter Wrong?, an occasionally successful attempt to do real-time fact checking on viral images and tweets. He tweets at @flashboy.

When Hurricane Sandy hit New York and New Jersey, I was running a blog called “Is Twitter Wrong?” an experiment at fact-checking viral images.

When a major natural disaster hits an area densely populated with heavy social media users - and media companies - one result is a huge number of images to sift through. Telling the good from the bad suddenly shot up the editorial agenda.

One particularly viral pair of images showed a shark supposedly swimming up a flooded New Jersey street. I teamed up with Alexis Madrigal from The Atlantic to try to verify these images.

One aspect of the images, shown below, is that they were strange enough to make you suspicious, yet they weren't implausible enough to dismiss out of hand. In the end, and they
proved very hard to definitively debunk.

Pre-existing images that have been misattributed (perhaps the most common form of “fake”) can often be debunked in a few seconds through a reverse image search. And pictures of major events can often be at least partly verified by finding mutually confirmatory images from multiple sources.

But neither of those work for a one-off chance sighting that’s either an original picture or an original hoax. (My experience is that verification of images that can't be debunked/verified within a few minutes tends to take a lot longer.)

In the end, sometimes there’s no substitute for the time-consuming brute force approach of image verification: tracing an image’s spread back through social media to uncover the original; walking the streets of Google Street View to pinpoint a rough location; and/or scrolling through pages of Google Image results for a particular keyword, looking for possible source images.

In this case, the Google Image search approach paid off - we were able to find the exact im-
age of a shark's fin that had been Photoshopped into one of the pictures.

But even then, we were unable to say that the other image was definitively fake. It used a different shark.

Our attempts to find the origin of both shark images kept hitting the barrier of people saying, vaguely, that it was “from Facebook.” We eventually found the originating Facebook poster via a tweet directing us to a news site that credited the source. (Both the news report and Facebook posts have since vanished from the Web.) But even that didn’t entirely help, as the page owner’s other photos showed genuine flooding in the same Brigantine, New Jersey, location. He also insisted in replies to friends that the shark pictures were real. (In retrospect, he seemed to be intent mostly on pranking his social circle, rather than hoaxing the entire Internet.)

The fact that he was claiming one undoubted fake as real was enough for us to move the other shark image into the “almost certainly fake” category. But we still didn’t know for sure. It wasn’t until the next day, when the fact-checking site Snopes managed to identify the source image, that we were able to make that call with 100 percent certainty. This was the shark image that was used to create the fake:

![Shark Image](Photo: Scott the Hobo)

That may be the main lesson from Sandy: Especially in rapidly developing situations, verification is often less about absolute certainty, and more about judging the level of acceptable plausibility. Be open about your uncertainties, show your work, and make it clear to the reader your estimate of error when you make a call on an image.