Title: Clarifying Questions
Challenge: Geolocation of deepfakes from images
Published Date: Monday 13 October 2025

Q: Can we answer part of the challenge? eg. specific types of location only?
A: You will need to deliver at least one work stream.

Q: With regards to the red/blue testing, what is the degree of detail required in the prediction/estimate from the Blue team? e.g. Is a country (e.g. United Kingdom) sufficient or is greater detail required (e.g. Yorkshire).
Q: Detection location on which level? District, city, street, GPS coordinate?
A: We have no specific requirement, the best available. Where location estimates may vary in accuracy, we would be interested in understanding "why".

Q: Do you want this to be UK focused or global?
A: Ideally global

Q: Are you interested in commercial tools or the full suite of open capabilities (incl OSINT techniques)?
A: WS1 is to test open source, WS2 could be OS or in house.

Q: Can you possibly comment on testing done so far?
A: No

Q: Assuming also you're looking at adversarial attacks and spoofing methods?
A: Yes we want to understand when people change background images.

Q: Do you have evaluation methodology or is this part of the market assessment?
A: This is part of the market assessment.

Q: No training models required right?
A: Yes, that is correct.

Q: What do you define as MVP?
A: The link challenge form details the MVP.

Q: So you want a commercially available geolocation tool that also highlights if the photo is not real/impossible to exist?
A: Yes, but they could be separate tools.

Q: With regards to "commercial photo geolocation tools", does this include ML models from sources such as GitHub or HuggingFace?
A: Yes, anything opensource.

Q: This is evaluation of commercial tool outputs?
Q: The first phase is evaluation?

A: Yes, this is the evaluation of all tools available.

Q: Applicants should aim to deliver a report of their research, and, if applicable, **a developed geolocation deepfake detection** image tool. This part was confusing.
A: These are two different workstreams, only deliver the one you can.

Q: Desirable requirements as well mentions you want "A geolocation tool which.." and details of the training data
A: In terms of the heat map, for example you could overlay a RAG status of confidence.

Q: Are you against improvements to existing tools (e.g. making models more robust to the things you mentioned you care about earlier), alongside evaluating and comparing existing models/tools?
A: We are more interested in improving detection than improving the tools.

Q: Could you clarify whether geolocation tools are expected to operate exclusively in offline mode during testing, or if both online and offline functionalities can be considered?
A: Both are considered in testing, the final product will need to operate offline.

Q: What is your current technology stack? Have you hosted the current solution on-premise or in Cloud? In either case, how would you provide the access to your test images that you had tested so far?
A: Test images are not provided.

Q: Can you explain more about the connection between the deepfake and geolocation strands? Do you see these are separate pieces or work?
A: They are separate workstreams but we would prefer them to work together.

Q: Is it more fully ai generated images you care about? Or AI-*edited* images (i.e. partial edits)?
A: Full and partial edits.

Q: Are there any preferred evaluation metrics (e.g. Accuracy, AUC)?
A: Any are considered

Q: - Beyond specialist tools, could more general "popular" tools such as ChatGPT be employed (E.g. "Geolocate this image?")?
A: Yes

Q: Under Project Scope, the wording specifies the delivery would be a report of the applicants' research, and, if applicable, a developed geolocation deepfake detection image tool - but the breakdown of the workstream does not mention any app or software development.
A: Not for WS1 but yes for WS2

Q: Could you please clarify whether as applicants we would only be performing tool/software testing and red/blue teaming, or would there be a mandatory requirement for the development of a tool/app?
A: WS1 would be evaluation and the judgement of the code.

Q: I wanted to confirm whether it is possible for a non-UK entity from the EU to lead or being a part of the team for the Geolocation and detection of deepfakes from photos challenge?
A: Organisations from outside of the UK and are not embargoed countries can apply.

Q: The co-creation links seem broken - surevine's server gives a 403?
A: We are aware of some bugs with our new website, you can navigate to the page here: https://co-creation.hmgcc.gov.uk/

Q: Are the personnel CV's required as pen profiles or as full two-page documents?
A: A summary of the technical credibility of those involved is sufficient.