

Document Details: Clarification Questions – Tracking a data footprint

Deadline for questions: 03/08/26

Publish Date: 06/08/26

1.0 Technical

	Question	Answer
1.1	Platform: capturing advertising-related tracking traffic is significantly more feasible on Android than iOS without enterprise-level device access. Is a single-platform (Android) Phase 1 prototype acceptable, or is cross-platform coverage expected even at this stage?	Focus upon Android is acceptable for this phase
1.2	Beyond existing tools such as TrackerControl, PCAPdroid and native mobile privacy reports, which capability or usability gaps are most important to address? Have particular limitations been identified through previous evaluations?	No specific capability gaps in mind, we wish to have as comprehensive a view as possible as to the Privacy exposure when using Apps
1.3	What decisions should the individual user or their security team be able to make using the demonstrator? Is the priority awareness, changes to app settings or	For the demonstrator we are seeking information only – specifically identification of what information is being revealed,

Official

	behaviour, identification of concerning exposure, or another outcome? Is active blocking expected, or is monitoring with actionable explanations sufficient?	both at the time and over time – to understand privacy risk exposure - no active blocking is required
1.4	The example describes identifying specific information transmitted, including identifiers and location. Must the demonstrator directly observe those fields, or is clearly labelled inference acceptable where encryption prevents inspection? Would distinguishing observed metadata, inferred associations and unknown payload contents meet the intended requirement?	For this phase of the demonstrator - distinguishing observed metadata, inferred associations and unknown payload content - would meet the requirement. However, our requirement is to have a comprehensive understanding of what is being revealed, and therefore would ask if a statement could be included as to what could be possible in later phases to better understand all payloads, increasing accuracy / certainty of understanding over time
1.5	Is a defined and validated subset of apps, protocols and advertising-related activity acceptable, provided limitations are explicit? Are browser tracking, first-party collection, device fingerprinting and system-service traffic all expected within the initial scope? Are there minimum expectations for identifying the originating app?	In terms of priority for phase 1, Apps would be the priority. Others, such as browser tracking, first-party collection, device fingerprinting and system-service traffic may be in later phases. An indication of the art of the possible around these other areas would be helpful in any responses
1.6	Which mobile operating systems, versions and device types are most relevant? Should the solution work on an unmodified consumer phone without root access, additional certificates or modified apps? Must it coexist with an enterprise VPN, managed work profile or mobile-device-management policy?	The most current Android operating systems are most relevant i.e. 13, 14 and 15. It would be preferable if the solution could work without root access, but not essential.

Official

		It will not need to co-exist with an enterprise VPN, managed work profile or mobile device-management policy.
1.7	Does this primarily mean combining observations across apps and time on one device, or supporting retrospective analysis across multiple devices or people? Is a numerical risk score expected, or would a clearly explained exposure dashboard with uncertainty indicators be sufficient?	This means combining observations across apps and time on one device. For the dashboard we are looking for something that a non-technical user would understand. Therefore a score alongside some explained exposure of why that exact score has been given would be useful.
1.8	Does the “no external servers” constraint permit ordinary forwarding of the phone’s existing network requests and controlled downloads of reference catalogues or software/model updates, provided no collected observations are uploaded? Is user-initiated export to a local file sufficient, and are there prescribed formats, retention periods, encryption or redaction requirements?	'No external servers' refers to a desire to not hold the outputs of this work on a public cloud. Normal interactions by the phone/network should continue. There are no prescribed formats, retention periods, encryption or redaction requirements at this time.
1.9	Our intended boundary is that any model inference or personalisation would occur entirely on the device. External AI assistance during development would receive only code, synthetic examples and non-personal reference material, not collected user data or personalised model updates. Are there additional sponsor requirements concerning local learning, model provenance, explainability, reset/deletion or validation?	Limiting data during development to synthetic data only is good to hear Use of AI within the solution itself should come with full explanation of what the data exposure, use, and any residual privacy & cyber risks are

1.10	Would an original evidence-analysis and user-interface component built around suitably licensed open-source capture technology fit the scope? Are there restrictions on open-source licences, background IP, or companion-app dependencies that applicants should address when distinguishing this approach from repackaging a third-party commercial system?	Yes, we are open to a variety of approaches to solve this problem
1.11	What environment and evidence will establish TRL 5 for this challenge? Are there expected thresholds for capture accuracy, attribution, reliability, battery impact or user comprehension? Can representative devices, users, test scenarios or reference datasets be made available early, and can acceptance criteria be agreed at project commencement? Is there a minimum starting TRL?	We would expect the proposer to outline what their 'definition of meeting TRL5' will be – including any constraints / limitations for a demonstrator We can discuss potential test scenarios and acceptance criteria prior to project commencement
1.12	May the one-page proposal include links to a short demonstration, source repository or test results, and would assessors consider those materials? I would retain all substantive proposal content within the stated page limit	No - we will not be clicking any embed links within proposals
1.13	Could you clarify the expected level of observability for encrypted advertising-related network traffic? Would a solution remain in scope where encrypted or certificate-pinned traffic is classified using observable on-device metadata — for example app attribution, destination/domain information, timing, connection	Yes - a solution could remain in scope where encrypted or certificate-pinned traffic is classified using observable on-device metadata / distinguishing observed facts from inferred data exposure where payload contents cannot be inspected

Official

	behaviour and other legitimately available signals — while explicitly distinguishing observed facts from inferred data exposure where payload contents cannot be inspected?	As mentioned in a previous answer, we would welcome comments / any novel suggestions of how to increase observability in later phases

2.0 Delivery

2.1	Whether there is any restriction on the use of third-party AI assistants during proposal development	We do not stipulate how or if potential solution providers use AI. It is completely at the solution providers own risk and choice
-----	--	---

Official

2.2	Whether there would be any restriction on the use of such tools during project delivery if funded?	We do not stipulate how or if potential solution providers use AI. It is completely at the solution providers own risk and choice
2.3	If there are conditions under which such tools may be used, what those conditions are?	We do not stipulate how or if potential solution providers use AI. It is completely at the solution providers own risk and choice
2.4	The application portal requires an Organisation Name and a 6–10 character Registration Number. Should a sole innovator enter their HMRC UTR, or is another identifier expected?	Yes the UTR is sufficient for a sole trader
2.5	Personnel: our team is based in India. If selected, would BPSS-equivalent checks be arranged for non-UK personnel, and does that affect eligibility to deliver the contract, not just to apply?	No security checks are required for this project – please check the information provided on the challenge form for any nationality/country restrictions
2.6	What does “Funding Party's sole use” mean? Is that HMGCC only, or does it include other Crown departments, agencies, contractors and international partners?	By reference to Definition “Funding Party”, Funding Party refers to HMGCC and/or Defence Science & Technology Laboratory (DSTL) acting on behalf of the Crown. For clarity, this is inclusive of offices, departments and agencies of the Crown, pursuant to Definition “Crown”, however does not extend to contractors or international partners.

Official

2.7	Can you confirm that clause 10.5 does not assign any Background IP or Project IP embodied in a Deliverable, and that ownership of such IP remains with the Solution Provider pursuant to clauses 10.1 and 10.2?	IP ownership remains with the Solution Provider pursuant to 10.1 and 10.2 – please note sub-clause [10.5] is to provide clarity that any usage licence will be assigned to the Authority, and not Cranfield.
2.8	Is the licence under clause 10.4 perpetual, and is it royalty-free after completion ?	Yes
2.9	Does the licence permit modification, copying or sublicensing of the software, or merely use of the supplied Deliverable?	Pursuant to clause 10.4, the licence is limited to use of the relevant Background IP and project IP solely to the extent wholly and necessarily required for use of the deliverables.
2.10	Can the Solution Provider identify Background IP expressly in the proposal/Contract Offer Letter and limit the licence to specifically identified components necessary to operate the demonstrator?	Yes, Solution Providers may identify any Background IP within their proposal and may specify reasonable limitations relating to their Background IP, however pursuant to clause 10.4 any such limitations must not restrict or prevent the Funding Party's use or benefit of the Project IP and Deliverables produced under the contract. The successful supplier(s) will be requested to provide and maintain a register of all relevant Background IP for contractual records, prior to commencement of delivery.

Official

2.11	Are there any UK establishment, residency or delivery-location requirements beyond the published eligibility conditions? Where can applicants find the expected payment milestones and rules governing subcontracting, test-device purchases and contingency within the £60,000 excluding-VAT ceiling?	The eligibility conditions published at the eligibility conditions applied to this challenge. The payment milestones are determined by the sprints and project plan proposed by the solution provider. The £60k budget is the budget set for this project any spend over and above this is at the solution providers discretion and will not be reimbursed. Test device purchases are to be included in the project plan as a budget unless the solution provider wishes to purchase at their own expense.
2.12	The supplied brief indicates a December 2026 project kickoff, while the challenge portal indicates November. Which should applicants use for staffing and delivery planning, and is the twelve-week period measured as consecutive calendar weeks?	December 2026.