



Challenge: Tracking a data footprint

Summary of the challenge

Can you help us minimise a person's data footprint?

The latest HMGCC Co-Creation challenge is seeking a mobile app which can help a phone user monitor this data over time.

This opportunity is looking for experts able to develop a mobile app to Technology Readiness Level 5 (TRL 5) within 12 weeks.

While some data on phones enable apps to function, other elements are used for tracking, profiling and personalising. This challenge is about working out how this impacts on a person's digital footprint.

The app should be able to:

- Enable a user to easily monitor their own data footprint exposure over time, enabling them to adjust their behaviour as necessary.
- Provide data to inform the management of aggregated risk to privacy sensitive individuals.

HMGCC Co-Creation will provide funding for time, materials, overheads and other indirect expenses for applicants successful in phase 2 of the competition.

Technology themes

App development, cybersecurity, data science and engineering, digital services, information technology, software development.

Key information

HMGCC Co-Creation will be hosting a two-stage competition process.

Phase 1. The objective is to rapidly assess one-page proposals. Those unsuccessful will be informed with feedback. Successful applicants will be invited to phase 2. For further information please see **How to apply – phase 1.**

Phase 2. Following a feedback phase, successful phase 1 applicants will be requested to submit a proposal directly to cocreation@hmgcc.gov.uk. For further information please see **How to apply – phase 2**.

Total budget (excluding VAT)	£60,000
Project duration	12 weeks
Phase 1 Competition opens	Monday 7 September 2026
Phase 1 competition closes	Thursday 24 September 2026
Applicants notified	Monday 5 October 2026
Phase 2 competition opens	Monday 5 October 2026
Phase 2 competition closes	Thursday 15 October 2026

Context of the challenge

When apps are installed on mobile devices, they can typically access certain types of information about a phone and how it is used. Core collection tools used are:

- Advertising IDs – a unique device specific code to track digital advertising.
- Advertising software development kits – code in apps that harvest data.
- Pixels and cookies – code trackers embedded in websites and mobile browsers that follow a user's behaviour.
- Device fingerprinting – combining technical details to uniquely identify a device without using cookies.

Types of data gathered include:

- Geolocation of the device.
- Device status such as IP address and battery level.
- Behavioural activities, such as which app is being used and for how long.

Although the information is usually anonymised, in practice it can often be linked to email addresses or phone numbers. Coupled with this, companies can sometimes sell or share this data with brokers who may then aggregate, build device-level movement histories, and resell this to advertisers.

For privacy sensitive individuals, such as those working in national security and defence, this creates a direct threat to their identity and safety.

This information may be exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to the originating department.

The gap

There are existing tools that can reduce data exposure, including VPNs, advertising blockers and privacy-first browsers. While these can be useful, some information is always needed to allow the app to work properly. This challenge is looking to minimise what is revealed and actively manage the aggregated risk of data exposure.

HMGCC Co-Creation is seeking a simple to use, on-device solution that enables a user to monitor their data exposure, that can:

- Capture as much advertising related information as possible.
- Aggregate the data into a simple understandable feed.
- Present a clear visual data exposure / risk dashboard.

Example use case

Gwen is an undercover officer. Most of her work is done from the passenger seat of a patrol car, sometimes for hours at a stretch. She needs a dedicated work phone so she can stay in touch with her team and receive emergency alerts, but she also needs to be sure the phone isn't a hidden back-door for hostile actors.

She has installed the new data-footprint tracker on her device. At regular intervals, she opens a single dashboard and instantly sees a colour-coded list of every app that has spoken to an advertising network, the time of each connection, and the type of identifier that was transmitted (for example device ID, location, OS version).

When she taps on a row, the app explains in plain English: "The 'NewsToday' app sent a request to 'ads.doubleclick.net' at 14:32, including your unique ID and approximate location. This is used to build a behavioural profile for targeted ads."

With this clear picture of her data footprint, she can see what data has left her phone and, if needed, contact her security team for advice.

Project scope

The focus of this challenge is to package mature techniques for monitoring advertising-tracking on internet connected devices, visualise the collected data, and deliver a user-friendly interface that can be interrogated by non-technical users.

The outcome, following the 12-week project, should be a demonstrator to a minimum Technology Readiness Level (TRL) 5 – technology basic validation in a relevant environment. The software should be demonstrated to the sponsors.

Essential requirements:

This information may be exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to the originating department.

- Capture advertising-related network traffic.
- Store data locally with no cloud upload and ability to export data.
- Present a clear, colour-coded dashboard on the phone.
- Include a description for each entry.
- Deliver a prototype that runs on a single common mobile operating system.

Desirable requirements:

- Provide a data export facility, to aid retrospective analysis of aggregated data.
- A prototype that runs on multiple common mobile operating systems.

Constraints:

- All processing must stay on the device – no external servers.
- No specialised hardware beyond a standard consumer smartphone.

Not required:

- Horizon scanning.
- Re-packaging of a third-party commercial system.
- Full commercial-grade hardening for large-scale deployment.

Dates

Phase 1 competition opens	Monday 7 September 2026
Clarifying questions deadline	Wednesday 16 September 2026
Clarifying questions published	Monday 21 September 2026
Phase 1 competition closes	Thursday 24 September 2026
Applicants notified	Monday 5 October 2026
Phase 2 competition opens	Monday 5 October 2026
Phase 2 competition closes	Thursday 15 October 2026
Applicant notified	Thursday 22 October 2026
Pitch day in Milton Keynes	Thursday 29 October 2026
Applicants notified	Monday 2 November 2026
Commercial onboarding begins*	Friday 6 November 2026

This information may be exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to the originating department.

Target project kick-off	December 2026
-------------------------	---------------

*Please note, the successful solution provider will be expected to have availability for a one-hour onboarding call via MS Teams on the date specified, to begin the onboarding/contractual process.

Eligibility

This challenge is open to sole innovators, industry, academic and research organisations of all types and sizes. There is no requirement for security clearances.

Solution providers or direct collaboration from [countries listed by the UK government under trade sanctions and/or arms embargoes](#), are not eligible for HMGCC Co-Creation challenges.

How to apply – phase 1

Please submit your application on the [HMGCC Co-Creation website](#). Any queries please email cocreation@hmgcc.gov.uk.

All information you provide to us as part of your application will be handled in confidence.

Applications **must** be no more than one page or one slide in length. HMGCC Co-Creation reserves the right to stop reading if this limit is breached. The page/slide limit excludes title pages, references, personnel CVs and organisational profiles.

Phase 1 applications will be assessed using the following scoring criteria:

Desirability	• How closely does the proposal directly address the challenge? ○ Does the proposal achieve all essential requirements? ○ How many desirable requirements are achieved? ○ Is this something the users want? • How well is the benefit for government and dual-use described? ○ Is the benefit to the users well described? ○ Have the applicants identified dual-use markets? • Ambition of the proposed solution? ○ Does the solution provide an incremental step in capability or significant leap?
---------------------	---

This information may be exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to the originating department.

	○ Does the solution introduce a new idea?
--	---

Following assessments, the successful applicants will be invited to submit a more in-depth proposal in phase 2. There will be feedback given to the successful applicants to aid their full proposal submission.

How to apply - phase 2

Applications **must** be no more than six pages or six slides in length. HMGCC Co-Creation reserves the right to stop reading after six pages if this limit is breached. The page/slide limit excludes title pages, references, personnel CVs and organisational profiles.

Phase 2 applications will be assessed using the following scoring criteria:

Feasibility	• What is the technical credibility of the minimum viable product proposed? ○ Is it technically possible? ○ Are there key technical risks overlooked? • Likelihood of the minimum viable product reaching or exceeding the minimum required Technology Readiness Level (TRL)? ○ Does the proposal aim to reach the minimum TRL? ○ Assessors' confidence in the proposal from technical perspective? ○ Will the proposal exceed the minimum TRL? • Credibility of the team regarding technical and project management skills? ○ Does the team have all the relevant expertise? ○ How experienced are they? ○ Have they delivered something similar before?
Desirability	• How closely does the proposal directly address the challenge? ○ Does the proposal achieve all essential requirements? ○ How many desirable requirements are achieved? ○ Is this something the users want? • How well is the benefit for government and dual-use described? ○ Is the benefit to the users well described? ○ Have the applicants identified dual-use markets? • Ambition of the proposed solution? ○ Does the solution provide an incremental step in capability or significant leap?

This information may be exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to the originating department.

	○ Is the proposed solution unique to the applicants?
Viability	• How well is the exploitation route described? ○ Is the proposal just aiming to deliver the minimum for the project? Or have they got a project plan post phase 1? ○ Are they thinking about commercial exploitation routes? ○ Are there rough costings for future work? • How well does the proposal demonstrate value for money and are the costs broken down and justified? ○ How much time and resource is spent on a project for the cost? ○ Is there a perceived high ambition for the cost? ○ Is there a robust costing plan? • How well is the project delivery described leading to the minimum viable product? ○ Is there a Gantt chart or similar? ○ Are there proposed outcomes after each sprint? ○ Are the applicants experienced in Agile methodology?
Budget	• Are the project finances within the competition scope?

Invitation to present

Successful phase 2 applicants will be invited to a pitch day, giving them a chance to meet the HMGCC Co-Creation team and pitch the proposal during a 20-minute presentation, followed by questions.

After the pitch day, a final funding decision will be made. For unsuccessful applicants, feedback will be given in a timely manner.

Co-Creation terms and conditions

Proposals must be compliant with the [HMGCC Co-Creation terms and conditions](#); by submitting your proposal you are confirming your organisation's unqualified acceptance of Co-Creation terms and conditions.

Commercial contracts and funding of successful applications will be engaged via our commercial collaborator, Cranfield University.

This information may be exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to the originating department.

HMGCC Co-Creation supporting information

[HMGCC](#) works with the national security community, UK government, academia, private sector partners and international allies to bring engineering ingenuity to the national security mission, creating tools and technologies that drive us ahead and help to protect the nation.

[HMGCC Co-Creation](#) is a partnership between [HMGCC](#) and [Dstl](#) (Defence Science and Technology Laboratory), created to deliver a new, bold and innovative way of working with the wider UK science and technology community. We bring together the best in class across industry, academia, and government, to work collaboratively on national security engineering challenges and accelerate innovation.

HMGCC Co-Creation aims to work collaboratively with the successful solution providers by utilising in-house delivery managers working [Agile](#) by default. This process will involve access to HMGCC Co-Creation's technical expertise and facilities to bring a product to market more effectively than traditional customer-supplier relationships.

FAQs

1. Who owns the intellectual property?

As per the HMGCC Co-Creation terms and conditions, project IP shall belong exclusively to the solution provider, granting the Authority a non-exclusive, royalty free licence.

2. Who are the end customers?

National security users include a wide range of different UK government departments which varies from challenge to challenge. This is a modest market and so we would encourage solution providers to consider dual use and commercial exploitation.

3. What funding is eligible?

This is not grant funding, so HMGCC Co-Creation funds all time, materials, overheads and indirect costs.

4. How many projects are funded for each challenge?

On average we fund two solution providers per challenge, but it does come down to the merit and strength of the received proposals.

5. Do you expect to get a full product by the end of the funding?

It changes from challenge to challenge, but it's unlikely. We typically see this initial funding as a feasibility or prototyping activity.

This information may be exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to the originating department.

6. Is there the possibility for follow-on funding beyond project timescale?

Yes it is possible, if the solution delivered by the end of the project is judged by the HMGCC Co-Creation team as feasible, viable and desirable, then phase 2 funding may be made available.

7. Can we collaborate with other organisations to form a consortium?

Yes, in fact this is encouraged, but within the maximum budget of the individual challenge.

8. I can't attend the online briefing event, can I still access this?

If a briefing event is held, any questions (and answers) will be captured and published after the event. The call itself is not recorded and use of AI notetakers is not permitted.

9. Do we need security clearances to work with HMGCC Co-Creation?

Our preference is work to be conducted at [OFFICIAL](#), we may however, request the project team undertake [BPSS](#) checks or equivalent.

10. We think we have already solved this challenge, can we still apply?

That would be welcomed. If your product fits our needs, then we would like to hear about it.

11. Can you explain the Technology Readiness Level (TRL)?

Please see the [UKRI definition](#) for further detail.

12. Can I source components from the list of restricted countries, e.g. electronic components?

Yes, that is acceptable under phase 1 - feasibility, as long as it doesn't break [UK government trade restrictions and/or arms embargoes](#).

Further considerations

Solution providers should also consider their business development and supply chains are in-line with the [National Security and Investment Act](#) and the National Protective Security Authority's ([NPSA](#)) and National Cyber Security Centre's ([NCSC](#)) [Trusted Research](#) and [Secure Innovation](#) guidance. NPSA and NCSC's [Secure Innovation Action Plan](#) provides businesses with bespoke guidance on how to protect their business from security threats, and NPSA and NCSC's [Core Security Measures for Early-Stage Technology Businesses](#) provides a list of suggested protective security measures aimed at helping early-stage technology businesses protect their intellectual property, information, and data.

This information may be exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to the originating department.

This information may be exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to the originating department.