Contribution ID: a4c15fea-2c43-4889-8c90-c76ea74a9268
Date: 13/05/2026 20:10:19

DMA.100220 - Consultation on the proposed measures for Alphabet to ensure interoperability with Android under Article 6(7) of the DMA

Fields marked with * are mandatory.

Introduction

The Commission is consulting third parties on the draft measures that Alphabet must implement to ensure effective interoperability with Artificial Intelligence (AI) Services on its Android operating system (Google Android), as required by Article 6(7) of the Digital Markets Act (DMA).

Target audience
All citizens, companies and organisations are welcome to contribute to this consultation. The Commission especially welcomes contributions from companies with first-hand experience on issues concerned by these proceedings, such as those providing Artificial Intelligence (AI)-powered services on Android smartphones and tablets or Original Equipment Manufacturers (OEMs) whose mobile devices are powered by Google Android.

Objective of the consultation

On 27 April 2026, the Commission addressed its preliminary findings to Alphabet, including the draft measures that Alphabet must take to ensure effective interoperability with Google Android.

The Commission is now seeking feedback from interested parties on the proposed measures. The Commission's measures cover four main themes and general measures for all features:

1. **Features for invocation.**
2. **Features for context.**
3. **Features for actions on apps and the operating system.**
4. **Features for access to resources (or the ability for AI service to use sufficient hardware and software resources to execute their tasks).**
5. **General measures for all features.**

More details about each of these features and the corresponding draft measures to ensure interoperability with Google Android can be found in the **Case Summary** and the **Annex containing the draft measures**, in the ***Reference documents*** section below (also available on the consultation page).

How to contribute

You can submit your contribution in response to this consultation through this form. You are not required to comment on each question. If your answer exceeds the character limit, you can upload your contribution as a PDF file through the field provided below.

The deadline to respond to this consultation is **Wednesday 13 May 2026**, 23:59 CEST.

Your submission must be fully NON-CONFIDENTIAL. All contributions will be made available to Alphabet. Contributions will not be published. The Commission may contact you with follow-up questions on your feedback.

Reference documents

Case summary - DMA.100220 - interoperability with Google Android

DMA.100220_-_Case_Summary_-_Google_Android.pdf

Annex (draft measures) - DMA.100220 - interoperability with Google Android

DMA.100220_-_Annex__draft_measures__-_Google_Android.pdf

Additional information

Contact

In case you have any questions, please contact EC-DMA@ec.europa.eu with "DMA.100220 - Consultation - Clarification question" as the subject line.
*This email address may **not** be used to send contributions.*

Protection of your personal data

The Commission **will share your response with Alphabet** to allow it to exercise its right to be heard under Article 34 of the Digital Markets Act, including your name/contact person, company/organisation, country, role within company/organisation and interest in the proceedings. However, the Commission will not share your email address with Alphabet.

Privacy Notice

DMA_specifications_consultations_privacy_notice_6-7_DMA.pdf

Your details

* Company/ organisation

Copper Horse Ltd

* Briefly describe your company / organisation

We are a cyber security company involved with consulting and designing future technology security for mobile, IoT, automotive and AI.

* Country

United Kingdom

* Contact person

David Rogers MBE

* Role within company/ organisation

CEO

* Interest in current proceedings - for instance, developing a specific AI service on Android, planning to offer a specific type of AI service on Android, device manufacturer, research activity in one of the areas concerned by the proceedings etc.

I am the former Chair of the mobile industry's Fraud and Security Group, I am working on security for defending future AI systems. I am concerned at the lack of consideration of security threats around spyware and other concerns.

* Email

david.rogers@copperhorse.co.uk

Your contribution

Please provide your input, in line with the instructions on the Public Consultation page. This input should address the draft **measures for Alphabet to ensure interoperability for Android mobile devices, to the benefit of third parties, including providers of AI services.**

Please mark in your response, to the extent possible, the specific measure(s) you are providing your feedback on.

I am a mobile phone security specialist and have been involved in mobile security for around 27 years. I am the former Chairman of both the GSMA Device Security Group and its parent group the Fraud and Security Group. I have and continue to conduct research into the cyber security of future technologies. This includes the defence of future AI security systems and have extensive experience in embedded mobile security technologies. I wrote and taught the Mobile Systems Security for MSc students at the University of Oxford as a part-time lecturer and served as a visiting Professor at York St John University, also teaching Cyber Security and Digital Forensics to undergraduates.

My concerns relate to all technical aspects of the draft measures including the effectiveness and completeness elements.

Whilst the intent of the work of the Commission is admirable, it cannot be taken on its own, without the context of the severe, hostile threat that all mobile devices and connected technologies face. In the two reference documents, there is only one mention of the word security, in the context of updates and only four mentions of the word privacy.

The market reality is that the mobile industry is under severe daily attack from a wide array of threat actors from the users themselves, to fraudsters, malware authors all the way up to private spyware companies and nation state actors. The mobile device is a hard target, but that is not an accident. It has been hard fought over many decades, with a continual cat and mouse game of malicious attacks and defence by the industry. This has led to the situation we have today, where the mobile device is a very secure object, with regular updates, industry reporting processes for discovering and resolving vulnerabilities and a robust ecosystem around application security including app ingestion and inspection. The industry is however still under continual attack and malicious actors are always seeking new ways to get into device and abuse legitimate features in order to achieve their aims.

One of the most pernicious types of attack that I spent a lot of time trying to disrupt in my time volunteering as chair at the GSMA, was that of private spyware. This involved many different aspects, both network and device / operating system related. Many different actions have been taken to tackle this problem across the world, including by industry, governments, the European Commission and journalist organisations. Some of my general observations and opinions from my experience in this area are relevant to this response:

1) Private spyware companies acquire and discover vulnerabilities through various means.
2) These organisations will stop at nothing to achieve their aims, including subverting companies, buying off individuals, setting up front companies, falsifying documentation etc.
3) They will target low-hanging fruit such as smaller third-party companies in the mobile industry supply chain that may have access relevant to their needs. Sometimes they will setup legitimate contracts with companies who don't realise what they are really doing.
4) The individuals involved will read lots of technical material, go to security conferences and work out where they can potentially create new exploitation of the technologies involved.
5) They will subvert technologies that are aimed at supporting disabled users (accessibility features) because they provide access to functions that normally wouldn't be provided – such as screen-reading, clicking and so on.

Many of these observations also apply to criminals involved in other areas where different types of malware are created, or where defrauding the user is the aim. Other abuse of the handset I have seen in the past has been targeted at creating mobile ransomware, abusing premium rate services or for data stealing purposes (which is then used as part of other crimes). The list is very long.

As an industry, we have seen the supply chain compromised time and time again, because it is a weak link and can be an easier target in some cases, because smaller organisations simply don't have the resources to face down, or even to detect the serious attacks that they will face when it comes to very serious threat actors.

Opening up sensitive user data to third-party organisations has to be done in a controlled and sensible manner. There are certainly some functions that are confined to the vendor of the operating system or to the manufacturer, simply because the risk of opening up would be so severe. That is not about a lack of interoperability, it just makes sound security sense.

In my view, the proposed measures open up the mobile attack surface considerably.

I had intended to go through line-by-line and give examples of where each draft measure could be abused, however this would be a very lengthy response! I am willing to speak to you and go through these in detail if you wish.

Do you have any other comments?

AI Attacks

I briefly also want to address the issue of the situation we find ourselves in, in 2026.

There has been a recent increase in autonomous AI systems which can go further than most human attackers would and more persistently. It is therefore now more important than ever to be a be able to control third party access to sensitive user data on devices.

The acquisition of information about users is a particular risk when it comes some spyware attacks, in some cases it has been fatal as has been widely (and in some cases, also not widely) reported. For those subject to the customers of spyware vendors, the draft measures being proposed are likely to be disastrous. Substantial effort by the mobile industry has gone into preventing such attacks. Spyware vendors will go to all lengths to get access to devices and will certainly seek to abuse third party access whether it be through front companies or other means.

At a broader level, the general acquisition of all and any information is of interest to companies using AI and building AI systems. The unscrupulous usage of that information may go undiscovered, but the intent is clearly there by various different actors and has been seen time and time again. What also makes the situation different in today's world is the speed and volume of data that can be processed. The pace of development of AI systems and in particular autonomous agents in the hands of malicious actors are of grave concern to everyone in the cyber security world.

It is therefore paramount that the current threat landscape and security environment is seriously considered before such measures are demanded. From reading the DMA Annex Measures, it is clear that only the functional, interoperability requirements have been considered, with little to no threat analysis. In my opinion, this is extremely dangerous for the cyber security of mobile devices in the future and has prompted my response to the consultation.

I do hope you will consider this feedback and as I stated above I am willing to speak to you about my detailed technical security concerns.

Upload your contribution

Alternatively, please upload here **one non-confidential PDF file** containing your contribution, along the themes and questions described above. The PDF should not contain any markings such as "confidential" or "business secrets".

Only files of the type pdf are allowed

☑ **I confirm that my contribution does not contain confidential information and understand that my contribution will be shared with Alphabet.**

Contact

Contact Form