13 May 2026

Feedback of

Association for Competitive Technology
(Transparency Reg. # 72029513877-54)
Square de Meeus 35,
1000 Brussels, Belgium

to the

European Commission

regarding the

DMA.100220 – Consultation on the proposed measures for interoperability with Google Android (Article 6(7) of the DMA)

I. Introduction

The Association for Competitive Technology (hereafter 'ACT') welcomes the opportunity to submit comments to the European Commission's consultation on the Google Interoperability measures under the Digital Markets Act (DMA).

ACT is a policy trade association for the **small business technology developer community**. Our members are entrepreneurs, innovators, and independent developers within the global app ecosystem that engage with verticals across every industry. We work with and for our members to promote a policy environment that rewards and inspires innovation while providing resources that help them raise capital, create jobs, and continue to build incredible technology. Today, the ecosystem ACT represents—which we call the app economy—is valued at approximately €95.7 billion and is responsible for more than 1.4 million jobs in the European Union (EU).[1]

II. Interoperability with Google Android

Interoperability, while important, should never compromise data security, encryption, and privacy. Interoperability is often accomplished via standards development enabling technical solutions for technologies to work together. However, the remedies proposed here go far beyond interoperability and past any measures necessary to address even the Commission's incomplete assessment of the marketplace. These proposed measures are wide-ranging and would reach deep into Android's inner workings, implicating cascading privacy, security, and usability issues on Android. As such, while this comment examines some of the proposed measures, the issues raised here are only illustrative and not exhaustive. With only two weeks to become aware of these proposed measures, analyse them, and formulate a response, this comment only responds to a representative sample of the proposed measures that would create serious problems for the artificial intelligence (AI) ecosystem.

The Commission's framing of this case positions the problem as one of large gatekeeper versus large AI challenger. With these proposed measures, the Commission seeks a comprehensive suite of API access obligations, contextual data sharing requirements, and resource allocation rules that would help a well-funded AI service to compete directly with Gemini across every major capability category.

This framing excludes the vast majority of Android developers from consideration. They depend on a secure Android ecosystem on which to build productivity apps, health tools, creative applications, accessibility services, and thousands of other products that rely on the stability, predictability, and security of the Android platform as it exists today. For these developers, the proposed measures represent not an opportunity but a source of uncertainty and risk.

[1] *See* 220912_ACT-App-EU-Report.pdf.

The Commission has not published any impact assessment specifically addressing how these measures will affect SME developers. Structural interventions designed to assist large actors can produce collateral damage for smaller actors. At this early stage in our review, it appears these proposed measures will result in serious harm to the Android ecosystem, including to small businesses that innovate on the platform. The Commission should postpone further steps in this case until the issues have been fully vetted with interested stakeholders.

Section 1: Measures for features on invocation

1.2 Measures for always-on hotword detection

The proposed measures on always-on hotword detection (AOHD) raise security and privacy concerns. The measure would require Android to support persistent background microphone monitoring for third-party services, including for user wake words, hotword detection models, and continuous DPS-level processing and microphone access. In practice, this would introduce permanent ambient listening, substantially increasing the risk of unintended data collection, possible exploitation, and reduced consumer trust. The Commission has not demonstrated how such access can be granted without undermining user trust, device security, and compliance with the General Data Protection Regulation (GDPR). These concerns should be properly assessed and addressed before imposing binding interoperability obligations.

Section 2: Measures for context

2.1 Measures for centralised access to apps' data stored on-device

The draft measures would apparently require Alphabet to support AppSearch for any third party. Under current conditions, Android enables a given app developer to provide a search function for on-device data stored by individual users within the app. For example, a health tracking app can use AppSearch to provide a feature for users to search across health parameters and dates for a given health outcome. However, the proposed measure in this instance appears to demand that Android enable third-party apps to access data stored by the health tracker app. Even with respect to apps dealing in less sensitive data, this would create serious privacy, security, and trust problems for developers. When a user downloads an app, they may agree to the developer's collection and processing of their personal information. In this arrangement, they should expect that developers safeguard their information and limit processing activities to those that are consistent with the context in which data was collected initially and decline to engage in processing or onward transfer that is not authorised, especially when such personal information is stored on-device. If Android must make this data available to any third party—including those for which a consumer is unaware of and has not consented to collecting any of their information—their expectations will be upset. Developers must be free to cultivate trust with their users and to keep their personal information secure against collection by third parties with which their users decline to share. The Measures for Context would force individual consumers and developers serving them to share data with unwanted third parties and this level of open access creates unnecessary privacy and security risks.

2.3 Measures for context-aware intelligence

In addition to mandating that Android make available passively collected information about a device owner's physical context to any third-party AI service (analysed further below), the Commission also proposes to require Android to provide all processing power available to Android's own services to any third-party AI service that demands it. The problem with this measure is simple: compute resources, and the battery power they consume, are finite. There appear to be no restrictions on the requirement to provide "hardware access and background execution (in particular selected and brought by the service) . . .." This raises the question of how Android must handle a deluge of requests for access to compute resources, including in the background, that exceed a device's capacity. Certainly, in such a case, Android may reduce its own compute resources in order to serve third-party requests with the same, lower capacity. This is likely to severely degrade the overall user experience, and make users reluctant to install apps in the future. Similarly, in cases where bad—or simply self-interested—actors seek outsized demands on compute resources that *can* be accommodated, there is nothing in these measures allowing Android to maintain capacity for smaller developers that do not meet the criteria for this provision and lack the resources to press their claims in Brussels. Likewise, nothing in the measures allows Android to take battery power, overheating, and other basic device usability factors that consumers care about into account. Usability is paramount for small businesses building on Android. Consumers are less likely to install apps if doing so can degrade the overall user experience, which would be especially harmful to SME app makers.

2.4 Measures for access to ambient data

The Commission proposes to require Android to provide any third-party AI service with continuous, background access to a device's microphone, camera, screen, and speakers, on equivalent terms to Alphabet's own first-party services.

The Commission notes that Alphabet's first-party services currently benefit from 'reduced consent processes and privacy indicators' for this access. The proposed remedy is to give third-party AI services the same reduced-consent, continuous access. Rather than raising the standard for all parties, the measures would normalise a surveillance-grade access model across a much larger set of actors, with no meaningful consideration of what this means for users, or for the developers whose apps sit on the receiving end of this data pipeline.

Any app installed on an Android device could, in principle, be monitored by a third-party AI service with ambient access to the screen. SME app developers have no control over which AI services a user installs, yet their users' interactions with their apps, including sensitive data entered into the app, could be continuously processed by a third-party AI system they have never consented to and with which they have no contractual relationship. Our members rely on the safe environment that platforms provide to keep bad actors out of the app ecosystem, gain consumer trust, and innovate. This provision, thus, may unintentionally hurt them by making the app ecosystem less secure and decreasing consumer trust.

The GDPR implications of this model are unresolved. If a third-party AI service processes personal data visible on the screen of an SME's app, questions of joint controllership, data processor

agreements, and lawful basis arise immediately. SME developers will face pressure from their own users and data protection authorities to account for processing they did not initiate and cannot prevent. The Commission should clarify such tensions before moving forward with the enforcement.

Section 3: Measures on features for actions on apps and the OS

3.2 Measures for screen automation

In this section, the Commission proposes to require Android to allow any third-party AI service to 'imitate user behaviour', 'autonomously control' installed applications, and run apps in virtual windows to complete tasks in the background.

The Commission offers no analysis of who bears legal responsibility when an autonomous AI agent takes a harmful action inside a third-party developer's app. If a third-party AI service makes an erroneous financial transaction, sends a private message without explicit user intent, submits a form with incorrect data, or triggers a purchase inside an SME developer's app, the liability framework is entirely unclear. SME developers will inevitably be drawn into disputes they played no part in creating.

Moreover, autonomous app control creates novel malware and fraud vectors. An AI service with screen automation permissions could, if compromised or deliberately misused, extract sensitive data from other apps, perform actions in financial or health applications without user knowledge, or serve as a persistent presence on the device that survives app deletion. The Commission's draft contains no security architecture requirements for AI services seeking screen automation access, and no minimum standards for auditability or sandboxing. Such issues should be clarified.

We urge the Commission to take these concerns seriously, engage meaningfully with the SME developer community before adopting binding measures, and design an interoperability framework that genuinely works for the full breadth of the ecosystem it purports to serve.

Sincerely,

Mike Sax
Founder and Chairperson

Maria Goikoetxea
Senior EU Policy Manager

Giulia Cereseto
EU Policy Manager