

Google, the EU, and the Right to Act

Apple made the authority problem visible. Google proves it was never an Apple problem.



THOMAS ROCHA III

JUL 16, 2026

Google, the EU, and the Right to Act

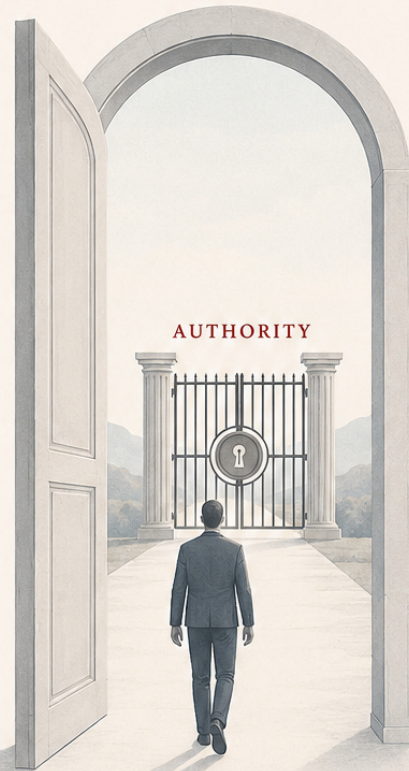
Apple made the authority
problem visible. Google proves
it was never an Apple problem.

Thomas Rocha III

July 2026

ACCESS

AUTHORITY



When the European Union pressed Apple to open more of its operating system to third parties, the argument could still be contained inside the familiar Apple frame.

Apple is closed.

Apple controls the device.

Apple uses privacy as both a design principle and a competitive wall.

Apple wants to decide which software may reach privileged system functions and which software must remain outside them.

That framing was never entirely wrong. It was simply too small.

On July 16, 2026, the European Commission issued two sets of binding specification measures to Google under the Digital Markets Act. One requires Google to give competing AI services equal access to eleven Android features relevant to AI assistants. The other requires Google to make specified Google Search data available to qualifying rival search engines, including AI chatbots with search functionality. ([Digital Markets Act](#))

Apple made the question visible.

Google removes the excuse that it was only an Apple question.

The Commission is no longer merely opening app stores, browsers, payment rails, or peripheral device interfaces. It is forcing the two companies that control the dominant mobile operating systems to admit rival AI services into functions through which software can act.

That is a different category.

An application displays information.

An agent changes the world.

It opens an app. It reads context. It invokes a service. It sends a message. It books a ride. It changes a setting. It retrieves a record. It initiates a transaction. It produces a result that another system may treat as final.

The old competition question was who gets access.

The new question is who has the right to act.

Google Is Not Being Told to Open a Door

The Commission says competing AI services must have the same access to relevant Android features as Google's own AI services. The measures concern eleven operating-system features, grouped into invocation, context, actions on apps and the operating system, and access to resources. ([Digital Markets Act](#))

That language sounds like access.

It is not merely access.

Read the feature list. Screen automation lets an outside agent imitate user behavior in a virtual window and complete multi-step tasks in the background. Structured on-device integration lets it act inside other applications, including Gmail, Calendar, Drive, Maps, and Messages. System integration lets it change device settings. Ambient data gives it the live sensor stream. Background execution lets it work while the screen is off.

A rival assistant that can be invoked by voice and can use system capabilities to search, book, communicate, or perform another task has not simply entered Android. It has entered the chain of action.

The distinction matters.

A browser asks the operating system to render a page.

An agent asks the operating system to help it produce an outcome.

The first is a compatibility problem.

The second is an authority problem.

Google can expose an interface. That tells the rival service how to reach a capability.

It does not answer whether the rival service is entitled to use that capability in this interaction, for this user, under this instruction, against this service, with these data, at this moment.

An API defines what can be called.

It does not define who governs the call.

The Commission Has Created a Contradiction Google Must Resolve

The EU wants rival AI services to compete with Gemini.

Google still has to protect Android users.

Those requirements do not cancel one another. Google is expected to provide meaningful interoperability while preserving cybersecurity, privacy, device integrity, and the lawful treatment of user data. The Commission's framework expressly allows security and privacy conditions around access to the most sensitive features. ([Digital Markets Act](#))

Google's own response makes the tension explicit. Its chief legal officer said the decisions risk undermining privacy and security protections for European users, and argued that the ruling grants external apps

powerful device permissions without existing vetting safeguards.
([Google](#))

Set aside who is right about the policy. Look at what the objection concedes.

Google is not arguing that rival agents cannot technically be admitted. It is arguing that admission without governance creates risk.

That is the correct diagnosis. It is also an argument Google cannot win by refusing to admit anyone, because the law now requires admission.

So the problem lands where it was always going to land.

Google must admit an outside agent without surrendering governability.

The rival agent must be real enough to compete.

Its authority must be limited enough not to become indistinguishable from platform compromise.

Google must not reserve all meaningful functions to Gemini.

Google also cannot treat every instruction presented by every rival agent as authoritative merely because the agent passed an eligibility review.

Certification Is Not Runtime Authority

Look at what the Commission actually built to hold the tension.

For five of the most sensitive features, Google may impose objective, nondiscriminatory eligibility conditions. Google must publish draft terms for the certification program by February 1, 2027, final terms by May 1, 2027, and must begin accepting applications on that date, with each assessment completed within four weeks. Independent third parties certify alongside Google. ([Digital Markets Act](#))

That is a real safeguard. It is also a static gate in front of a live problem.

Certification is not runtime authority.

Identity is not runtime authority.

An approved developer account is not runtime authority.

A permission granted last month is not necessarily authority for the action occurring now.

A certified agent is a trusted agent. A trusted agent is not thereby an authorized action.

The certification program answers whether this agent may generally be admitted to this class of capability. It does not answer whether this instruction, in this interaction, under this user's grant, against this service, at this moment, is within the authority actually conveyed.

The platform needs something that can decide that during the interaction.

Not whether the agent is generally trusted.

Whether this act is permitted now.

This Was the Missing Category in the Apple Argument

Apple's instinct was easier to understand because Apple's platform is visibly centralized.

If a third-party agent can act across files, messages, payments, applications, settings, health information, and personal context, something has to stand between that agent and the device.

Apple's answer appeared to be some form of trusted system intermediary.

The EU's concern was equally obvious. If Apple alone controls the intermediary, then the intermediary becomes the next gatekeeper.

Apple says the layer protects the user.

The EU says the layer may preserve Apple's market position.

Both can be true.

What was missing from the argument was a clean description of what the layer must govern.

Google now faces the same question under a different operating model.

Apple can concentrate the work inside a trusted operating-system agent, using hardware security, system mediation, entitlement, and local processing. Google can distribute it among Android permissions, service interfaces, security qualification, policy engines, identity systems, and audit records.

The architecture can look different at every visible layer.

What cannot differ is the requirement imposed by the problem.

A rival agent enters.

The user grants some authority.

The agent invokes a platform function.

The function reaches another service.

The service may mutate state.

The result returns through systems controlled by several different parties.

Somewhere in that process, the system must preserve the distinction between capability and authority. The governing authority must survive every change inside the interaction without originating a second independent authority root.

Otherwise, everything that can act eventually becomes entitled to act.

That is not an Apple design preference.

It is not a Google product choice.

It is the constraint created when regulators require open agency while leaving responsibility attached to the platform.

The Old Stack Can Still Perform the Task

Google does not need a new architectural primitive to make an assistant book a ride.

The old stack can do that.

Authenticate the user.

Issue a token.

Call an API.

Pass context.

Receive a response.

Write logs.

Return the result.

The task completes.

That is why this problem remained hidden for so long.

The old architecture can execute the action.

What it cannot do coherently is prove the authority of the action across the entire sequence.

Google may prove that Android admitted the assistant.

The assistant provider may prove that its model received a user instruction.

A mapping service may prove that its API was called with a valid credential.

A ride service may prove that a booking was created.

A payment provider may prove that the payment instrument was accepted.

Every record can be locally correct.

The assembled process can still lack a single defensible answer to the only question that matters:

Under whose continuing authority did the interaction mutate from request to completed state?

Logs show that events occurred.

They do not, by themselves, establish that the same governing authority survived them.

Transport preserves the connection.

Authentication identifies the actor.

Permissions define a possible scope.

None of those necessarily governs the live interaction as it changes.

That is the category the industry has not historically maintained.

Search Data Creates the Same Problem at a Different Boundary

The second Commission decision concerns Google Search data.

The DMA requires Google to share anonymized ranking, query, click, and view data with qualifying third-party search engines on fair, reasonable, and nondiscriminatory terms. The decision expressly makes AI chatbots with search functionality eligible to receive that data, and sharing is scheduled to begin in January 2027. ([Digital Markets Act](#))

This looks like a data-access dispute.

It is also an authority dispute.

The data did not appear from nowhere.

It was generated through interactions among users, queries, rankings, clicks, websites, advertisers, services, and Google's own infrastructure.

When that data crosses into another company's search or AI system, the relevant question is not only whether it was anonymized.

It is what authority accompanies the transfer.

Who may use it?

For what purpose?

For how long?

May it be recombined?

May it train another system?

What restrictions survive the crossing?

What happens when a downstream system derives a new result from it?

Which record proves that the use remained within the authority under which the data was provided?

The Commission can define eligibility, pricing, anonymization, and the required scope of disclosure.

Those are necessary rules.

They do not themselves create the runtime architecture that carries the rules with the data.

The rule sits beside the transfer unless the system binds it to the transfer.

That is the same failure seen elsewhere.

The policy exists.

The interaction moves.

The proof remains behind.

This Will Not Stop at Mobile Operating Systems

The Commission's decision is about Android and Search.

The architectural requirement is not.

The same pattern appears wherever an outside agent is allowed to act inside infrastructure controlled by another party:

cloud platforms;

enterprise software;

communications systems;

financial services;

healthcare systems;

vehicles;

industrial equipment;

public infrastructure;

edge networks;

machine marketplaces.

Every one of those systems can continue operating through fragmented credentials, local permissions, event logs, and after-the-fact reconciliation.

Every one of them encounters the same failure when the requirement becomes proof rather than performance.

Did the system do the thing?

That is easy.

Was the system authorized to do the thing, under the applicable conditions, throughout the interaction in which the thing was done?

That is the harder question.

Regulators are arriving at it from different directions.

Privacy calls it continuing validity.

Cybersecurity calls it bounded privilege.

Competition law calls it nondiscriminatory interoperability.

Accessibility calls it entitlement during the interaction.

AI governance calls it accountability.

Financial systems call it mandate and settlement.

They are not separate architectural problems.

They are different legal vocabularies for the same missing layer.

The Missing Layer Has a Name

It is called SSOAR: Session-Scoped Orthogonal Authority and Routing.

Authority that survives mutation.

The first embodiment issued on June 16, 2026 as U.S. Patent No. 12,659,408, Hermes-Echo, all twenty claims. It has nine siblings. They extend the same constraint to admission, participation, handoff, merge and fork, compute placement, provenance, residency, trust, and machine action.

The rest is at hermes-echo.com.

The EU Thinks It Is Opening Android

It is doing something larger.

It is creating a legally protected right for one company's agent to act through another company's platform.

That right cannot remain an abstraction.

Google must make it operational.

To make it operational, Google must determine who is admitted, what authority is granted, which constraints remain attached, how far the authority travels, when it ends, and which resulting state may be accepted as authoritative.

Apple must answer the same questions.

So will everyone downstream.

The industry can continue describing the answer as permissions, trusted agents, interoperability, orchestration, policy enforcement, identity, audit, provenance, or runtime safety.

Those are the pieces.

The missing category is the thing that makes the pieces one governed interaction.

Google has until August 1, 2027 to implement.

Apple made the right-to-act problem visible.

Google makes it systemic.

The EU is no longer merely opening platforms.

It is forcing the industry to build the authority layer between access and action.