It’s getting personal.

How abuse of the DMA’s interoperability mandate could expose your private information

December 2024

At Apple, we love empowering developers to build great apps for our users.

When it comes to new products and features, Apple's approach is always the same. We innovate to create experiences that our users will love. And we work to protect their privacy and security every step of the way. We also provide our developer community with a constantly expanding set of tools, technologies, and resources that allow them to build incredible apps on our devices. Apple has invested billions of dollars to develop amazing products and features that developers have used to create extraordinary things, including very successful businesses of their own.

This commitment to our developers is a fundamental part of Apple's DNA. We have pioneered approaches, for both developers and ourselves, that enable amazing user experiences without any company—including Apple—gaining access to users' private data. This is the foundation for user trust, and part of what enables success for everyone: users, developers, and Apple.

Apple has created more than

250,000

application programming interfaces, or APIs. APIs are tools that allow developers to make use of the incredible functionalities we've built.

Apple's commitment to developer success through interoperability that preserves privacy

Our users deserve a complete and transparent understanding of why a developer wants access to important parts of their devices, what that developer will do with it, and when it's happening.

Microphone

When we opened up developer access to the microphone on iPhone, allowing them to listen to what a user is saying and doing, we kept the user in control. Developers must ask users for their permission to access the microphone, and they must tell users when they are using that access to record audio.

Touch ID

Introduced in 2013, Touch ID is the first popular and easy-to-use biometric access smartphone technology. When in use, Apple keeps users' fingerprint data in iPhone's Secure Enclave, where not even Apple can access it. The Touch ID API for developers was released in 2014, so developers of banking apps, gaming apps and more can use this technology while preserving security and privacy of the user.

But we are now seeing concrete examples of how **a new approach to interoperability in the EU would put users at risk**, requiring them to open their devices—and their most sensitive data—to companies with a track record of violating their privacy.

The magical experiences people love about Apple products are made possible because of the time, talent and capital the company dedicates to creating products that work right out of the box.

These processes will hurt innovation—companies should be able to compete with one another to make their own products work together in new ways that benefit users without giving their ideas away to competitors. Apple is the only company being forced to share its innovations in this way with everyone else, including those who do not share its commitment to user privacy.

Interoperability risks

The Digital Markets Act commenced earlier this year, establishing in law the concept of "interoperability." The basic idea is that developers should have access to the same tools in iOS and iPadOS as Apple, in order to ensure a level playing field. Apple has always believed in that level playing field. As we continue to create opportunities for interoperability, it remains incredibly important to do so in a way that's right for our users. **That is why, every single time we open developer access to functionalities, we give careful thought to how to do it in a way that continues to protect users.** We all know the risks. Without the right protections, giving third parties access to parts of users' devices could open up ways for bad actors to steal or expose their personal information.

Today, as devices become ever more personalized, it's extremely important to keep user protections at the center of everything we do. Apple goes to great lengths to design software to protect the privacy and security of users. We are concerned that some companies—with data practices that do not meet the high standards of data protection law held by the EU and supported by Apple—may attempt to abuse the DMA's interoperability provisions to access sensitive user data.

Data-hungry companies across the globe may weaponize interoperability

As we strive to comply with the DMA, we carefully review each interoperability request we receive. As an example of our concerns, Meta has made 15 requests (and counting) for potentially far-reaching access to Apple's technology stack that, if granted as sought, would reduce the protections around personal data that our users have come to expect from their devices.

Some of the sensitive technologies Meta has requested to access

No company has made more interoperability requests of Apple than Meta. In many cases, Meta is seeking to alter functionality in a way that raises concerns about the privacy and security of users, and that appears to be completely unrelated to the actual use of Meta external devices, such as Meta smart glasses and Meta Quests.

- AirPlay
- App Intents
- Apple Notification Center Service
- CarPlay
- Connectivity to all of a user's Apple devices
- Continuity Camera
- Devices connected with Bluetooth
- iPhone Mirroring
- Messaging
- Wi-Fi networks and properties

If Apple were to have to grant all of these requests, **Facebook**, **Instagram**, and **WhatsApp** could enable Meta to read on a user's device all of their messages and emails, see every phone call they make or receive, track every app that they use, scan all of their photos, look at their files and calendar events, log all of their passwords, and more. **This is data that Apple itself has chosen not to access in order to provide the strongest possible protection to users.**

Apple collects only the personal data strictly necessary to deliver a product or service, we put the user in control by asking them for permission before apps can access sensitive data, and we provide clear indications when apps access certain sensitive features like the microphone, camera, and the user's location. We process data on the device, wherever possible, rather than sending it to Apple servers, to protect user privacy and minimize data collection. Third parties may not have the same commitment to keeping the user in control on their device as Apple and may prefer to move user information to their servers—where they can combine, profile, and monetize an individual's private data.

Third parties may not have the same commitment to keeping the user in control on their device as Apple

The General Data Protection Regulation (GDPR), which Apple has always supported, set a strong set of privacy rules for all companies to comply with. The DMA was not intended to provide a way around the rules. But the end result could be that companies like Meta—which has been fined by regulators time and again for privacy violations—gains unfettered access to users' devices and their most personal data. If Apple is forced to allow access to sensitive technologies that it has no ability to protect, the security risks would be substantial and virtually impossible to mitigate.

Messaging

Meta wants to access users' SMS and iMessage capabilities to send and read users' messages themselves. Separately Meta also wants to access their message history. Access to private communications needs to remain fully under the control of users.

AirPlay

For years, Apple has supported apps being able to send content via AirPlay. Meta is requesting direct access to users' TVs and smart speakers, which creates a new class of privacy and security issues, while giving them data about users' homes.

App Intents

Meta wants access to all of the data provided by other apps for App Intents, a new framework for managing how users interact with the apps and features on their devices. Such access would potentially provide Meta with the ability to fully control a user's device.

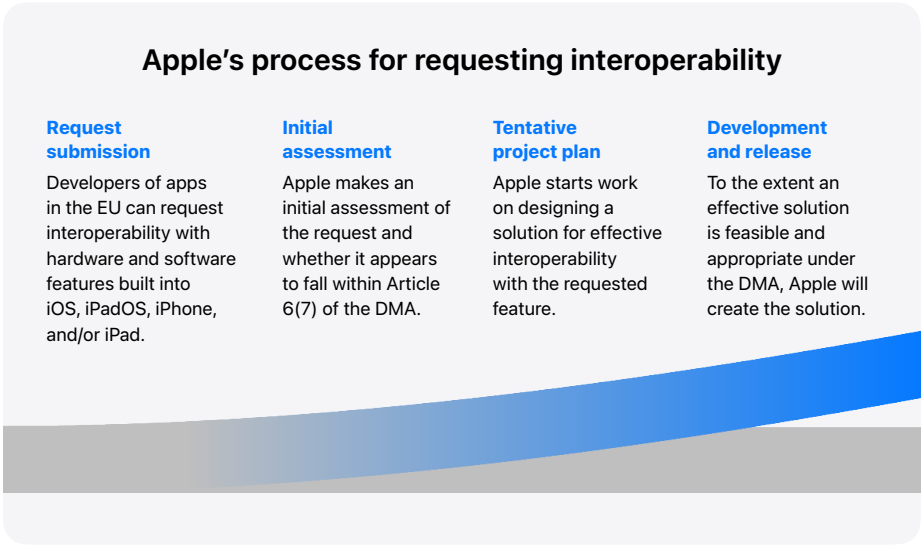
For instance, if a user asks Siri to read out loud the latest message received via WhatsApp, Meta or other third parties could indirectly gain access to the contents of the message. No one is in a position to understand the full risks of that.

CarPlay

Meta wants access to CarPlay functionality so that it can wake iOS apps and project additional content from user devices. This removal of control from users could undermine their choices.

Apple’s commitment to interoperability

We work diligently to review all requests and implement them when possible, taking into account the need to protect privacy and security on the platform. Even when the requests create serious risks like we have shown here, we are investigating enhancements to our platform that will enable richer experiences while continuing to protect sensitive user data and maintain device security. Our commitment is to evaluate and respond in a timely manner to all requests, ensuring the integrity of the platform is preserved for all developers and sensitive user data is protected.



Apple evaluates each request and keeps developers informed of the progress after a request is submitted. If at any stage of the process Apple determines that it’s not feasible to design an effective interoperability solution or that it is not appropriate to do so under the DMA, we communicate that to the developer.

Apple’s high standards for privacy and security are what set us apart.

Our users depend on it. We want users and developers alike to benefit from the great features and functionalities of iPhone—safely.

We will never abandon our bedrock commitment to our users’ privacy and security. We trust that the EC will seek to implement the interoperability requirements in a manner that respects the GDPR.