15 January 2025

EUROPEAN COMMISSION
BRUSSELS, BELGIUM

This is a response made as an individual expert on the EC's proposed interoperability measures in Case **DMA.100203**. Information on my background and relevant expertise is available at my website: https://www.ianbrown.tech/about/

For transparency, I have been commissioned by Meta Platforms Inc. to write an independent expert report on the security, privacy and integrity implications of the EC's proposals in this case and Case DMA.100204, which will be published in early February. This consultation response has been informed by the first part of that work, as well as discussions with other interested experts, but is entirely my own.

I applaud the Commission's comprehensive approach to addressing Apple's iOS obligations under the DMA's Art. 6(7) relating to connected hardware, such as smart homes and cars, an area of central importance to Europe's near-term digital society. It is critical for European competitiveness, innovation and protection of fundamental rights that EU consumers have a meaningful choice of these devices, rather than being tied to those from gatekeepers.

The Commission's proposed measures are narrowly and carefully drawn to enable Apple to comply with the DMA 6(7) obligation and so provide fair and non-discriminatory iOS treatment of third-party connected devices. They are a good example of how careful, case-by-case analysis can maintain the security, privacy and integrity of a DMA-designated operating system (OS) or virtual assistant while opening related markets up to fair competition.

iOS and other Apple OSes are carefully designed to reduce security, privacy and integrity risks, with a whole range of protective technical mechanisms. These are used to protect Apple's own services, devices and apps, and with care can also be used to enable interoperability with third-party software and devices while continuing to protect end users. As the Commission's consultation document importantly notes:

> *“An integrity measure pursuant to Article 6(7) second subparagraph of Regulation (EU) 2022/1925 cannot be considered strictly necessary and proportionate if it seeks to achieve a higher level of integrity than the one that Apple requires or accepts in relation to its own services or hardware.” (131(e))*

In the table shown on page 6, I have preliminarily mapped the specific technical changes enabling the measures proposed by the EC[1] to be implemented on iOS to a scale of potential risks to security, privacy and integrity (colour-coded according to the table on page 7). These potential risks are based on possible vulnerabilities introduced, such as access to user data or system resources by malicious software, or undermining user choice over third-party access to resources such as a phone’s microphone or Bluetooth connections.[2]

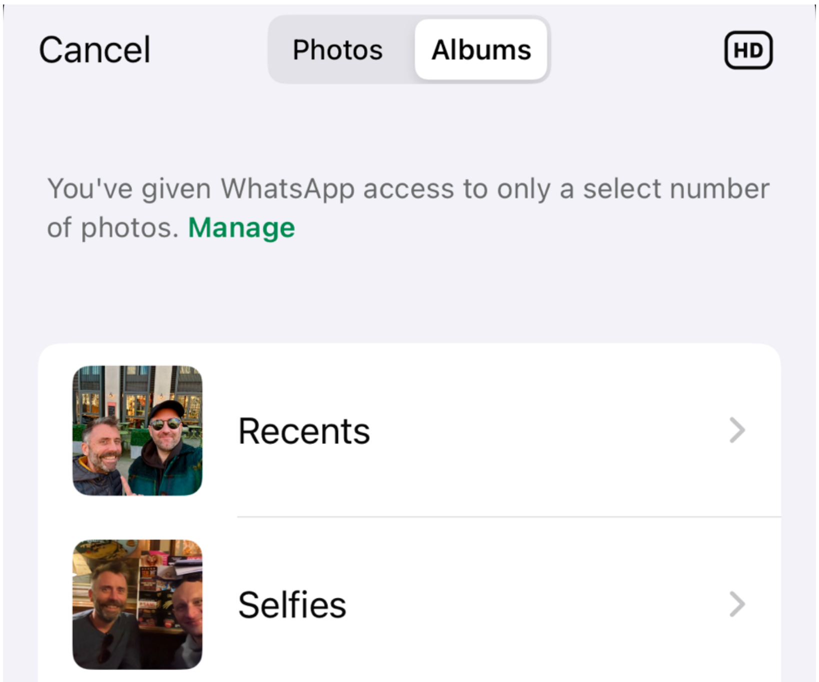
My assessment is that the EC’s proposed measures present lower to medium-level risk, which can be managed using iOS’s existing technical controls, extended as appropriate; legal requirements for third-party compliance with European law (such as the GDPR); and iOS user interface measures to ensure users provide informed permission for third party devices to interact with specific features of their systems.[3] For example:

[1] Numbers in the table cells refer to [paragraph]/(sub-paragraph) numbers in the EC proposed measures. Three non-cross-cutting measures are also proposed: **Notifications** [1.1] Access to notifications (3), including Apple Push Notification Service and capability for notifications to be sent directly to connected devices from a server, "without passing through the iOS device” (EC para. 2) — although clearly that means a device would need its own connectivity; **Proximity-triggered pairing** [1.9] Bluetooth Pairing (103e); Accessible registry of devices, BLE adverts, and metadata (107); **Automatic Wi-Fi connect [1.10]** Bluetooth Pairing Implied by (113).

[2] These are two of several examples given by Apple in its December 2024 response to the DMA’s interoperability requirements, It’s getting personal – which lacks the required level of detail to justify its claims.

[3] As the parallel Case DMA.100204 proposed measures notes, recital 50 of the DMA can also be used as guidance: “*In order to ensure that third-party software applications or software application stores do not endanger the integrity of the hardware or operating system provided by the gatekeeper, it should be possible for the gatekeeper concerned to implement proportionate technical or contractual measures to achieve that goal if the gatekeeper demonstrates that such measures are necessary and justified and that there are no less-restrictive means to safeguard the integrity of the hardware or operating system. The integrity of the hardware or the operating system should include any design options that need to be implemented and maintained in order for the hardware or the operating system to be protected against unauthorised access, by ensuring that security controls specified for the hardware or the operating system concerned cannot be compromised*”.

1. Over the last several versions of iOS, Apple has been adding capabilities for users to limit app access to certain categories of data to specific items, using user interface tools built into the OS – for example, files, photos, and most recently contacts, as shown in this screenshot:



You've given WhatsApp access to only a select number of photos. Manage

2. iOS includes mechanisms for apps to perform very specific functions while they are not currently running in the foreground (interacting with the user), such as to play audio or video, or check whether a timer has expired.[4] This type of functionality could be extended to the specific new background capabilities required by the EC's proposed measures, while protecting the integrity of iOS.
3. Apple has been moving towards a (much) more secure model of OS execution of code to interact with hardware devices ("device drivers"), with most such code now running (like applications) in the controlled "user space" of the OS, rather than the (much less controlled) "kernel". The EC's proposed measures would not require Apple

[4] Discussed in an Apple developer support post, iOS Background Execution Limits.

to allow third-party code to run in the iOS kernel.[5] And for the higher-layer protocols the EC is proposing Apple make available to third-party code (such as AirDrop, AirPlay, peer-to-peer Wi-Fi and Core NFC), this can be done using safe user-space technical interfaces (APIs).

4. iOS isolates data it receives via Messages and its Apple Identity Services, using a service called BlastDoor. It is not clear if iOS also applies this to files shared using AirDrop, but this would be an additional protection for data received via this route, or for iOS to apply to other AirDrop-like services.
5. iOS communications protocols including Wi-Fi and Bluetooth support the use of temporary identifiers, to reduce the possibility of third parties tracking iOS devices over time. This functionality could also be supported for third-party devices connecting to iOS peer-to-peer Wi-Fi,[6] and in AirDrop-like services.
6. iOS also supports the latest versions of communications security protocols such as Transport Layer Security (TLS), which again could protect third-party device communications using peer-to-peer Wi-Fi and other types of networking links.

Apple may be required to undertake significant development to comply with some interoperability requests (as described in para. 55 of the accompanying Case DMA.100204), with a correspondingly long compliance period (12 months). Future functionality developed in iOS available to Apple's services must be designed to be interoperable from the start, and to comply with European data protection and cybersecurity laws. In both cases, this functionality should be designed to be explicitly security and privacy-protective, with access to minimal iOS resources (e.g. personal data) for a specific purpose.[7]

[5] By contrast, Microsoft still allows certain third-party code to run in the Windows kernel. This was behind the worldwide IT outage caused by CrowdStrike security monitoring software in July 2024.

[6] It would arguably be better for system security for Apple to adopt the industry-standardised Wi-Fi Aware protocol, which would enable greater scrutiny and testing/analysis by third parties.

[7] An example of such a protocol is described in Operating Systems need privacy-protective friend-finding services.

For each of the required technical changes I have identified in the table on page 6, I have also noted appropriate iOS technical controls to manage the risk of those changes (shown in the second row). Where these controls required adaptation to protect newly-interoperable functionality, this would be a justification for Apple taking the longer of the two periods the Commission has proposed in its accompanying consultation (Case DMA.100204 para. 55).

It is possible to envisage other types of interoperability access which *would* threaten the integrity of an operating system, shown in the right-most sections of the table on page 7. But these measures have *not* been suggested by the European Commission in this consultation.

The use and continuing development of iOS technical security controls will enable Apple to follow the Commission's proposed interoperability measures without threatening the integrity of its smartphone operating system, or the security or privacy of its users. Apple's commitment to the latter is a great example of the approach required by European laws such as the General Data Protection Regulation. We can but hope it will take a similarly positive attitude to the Digital Markets Act in future.

I would be pleased to answer any questions or provide any further information which would be helpful to the Commission's final decision on their proposed measures in this case.

SINCERELY,

DR IAN BROWN

Functionality for third-party code (to the same level as Apple's own devices)		Background execution	Access to service-specific data	Identify "Trusted" devices/ contacts	Access iPhone P2P Wi-Fi	Discover nearby devices/be discoverable	Standardised protocol	Bi-directional file-sharing
Applicable/potential iOS controls (all would require user consent, use protective mechanisms equivalent to Apple devices, comply with GDPR, Cybersecurity Act etc.)		Resource consumption limited	Data minimised; temporary identifiers	BlastDoor and Apple Identity Services-like functionality; Bluetooth secure pairing	Address randomisation; TLS support	Address randomisation	Support for address randomisation, data security	BlastDoor-like data checking
Feature/EC proposed measure								
Interactivity	**Notifications** [1.1]	Implied for companion app (7a)						
	Background execution [1.2]	(14); (15) for sister and companion apps/relevant processes				(14)		
	Automatic audio switching [1.3]		(23) for audio-switching data					
Data transfers	**High-bandwidth P2P WiFi** [1.4]	(32g)			(31)	(32a)	Give access to AWDL (36) or use Wi-Fi Aware (38)	
	Airdrop [1.5]			(57)	(48)	(48/49) (including via "BLE, NFC, or P2P Wi-Fi")	Provide AirDrop protocol spec. (45)	(52)
	Airplay [1.6]	(71/implied by 73?)			(73)	(71/72)	Provide AirPlay protocol spec. (71)	
	Close-range file transfer [1.7]	Implied by (81b), (83d), (84c); explicit in (87)		(81c), (83e), (85) incl. via contacts database	(80), (84a), (86)	(80), (84c)	(81d)	(80)(83d)
	Media casting [1.8]	Implicit in (95); explicit in (96f)			(96d)	(96c)	Implied by (96b)	
Device setup/ configuration	**Proximity-triggered pairing** [1.9]	Implied by (105e)			(108)	Implied by (104),(105a-c)	Implied by (104), mentioned in (108)	
	Automatic Wi-Fi connect [1.10]		(114) "Wi-Fi Network Info"	(113)				
	NFC read/ write [1.11]						(123) Core NFC, 124(a)	

Security/privacy/integrity risk of enabling authorised third-party code to bypass specific operating system controls for interoperability purposes

Notes: 1. This table maps diverse risks onto a 1D scale and is by definition high-level and broad, given the broad range of potential threat models faced by an operating system.
2. The focus is technical risk, but particularly for privacy controls, legal compliance (eg with DMA, GDPR, cybersecurity law, and contractual limits) will play a role. Existing and expanded hardware/OS technical controls can be used to manage these risks, alongside legal and organisational controls, and user interface choices to gain full user consent.
3. Broad concepts of "kernel" and "user-space" are used here, but Apple's recent chips and OSes have more granular distinctions, such as the split "Secure Page Table Monitor and Trusted Execution Monitor" functionality (and Windows has a "secure virtual mode") which can protect even against kernel compromises.

<—Lower	Medium	High	Higher	☠ Highest—>
Highly granular, user-permissioned app capabilities designed to be explicitly security and privacy-protective, with access to minimal resources for a specific purpose (such as connecting (with their permission) with specific existing contacts on a new service[1])				
Granular, user-permissioned app capabilities closely controlled & monitored by OS, running in user-space				
User-permissioned app access to specific data items (eg specific files/folders, contacts, message senders/threads, photos/albums), ideally read/add-only, optionally excluding sensitive data elements (eg location)				
	Apps given user-permissioned access to entire collections of specific user data items eg files, contacts, photos, messages			
	Apps given access to service history data, such as IDs of previously seen WiFi APs/Bluetooth devices, with use of temporary identifiers where available			
		Apps can bypass certain app store checks		
			V limited and pre-checked kernel access for essential elements of device drivers, with most code running in user space; access to whole filesystems. NB Apple OSes are moving to user-space drivers built on DriverKit, with MFI checks on others	
			Broad, direct third-party code access to core system (kernel/hardware) Improved cybersecurity policy would push OSes away from this (see Windows/CrowdStrike[2]), as Apple is doing	
				Difficult to imagine a scenario where highest-risk measures would be proportionate to mandate Eg direct access to secure enclave rather than via carefully limited APIs

[1] See eg https://www.ianbrown.tech/2024/10/04/2074/

[2] See https://cheriot.org/security/philosophy/2024/07/19/crowdstrike-is-the-opposite-of-cheriot.html