



EUROPEAN COMMISSION

***CASE DMA.100203 – Article 6(7)
– Apple – iOS – SP – Features for
Connected Physical Devices***

(Only the English text is authentic)

**Digital Markets Act
Regulation (EU) 2022/1925 of the European Parliament
and of the Council**

Article 8(2) Regulation (EU) 2022/1925

Date: 19/03/2025

This text is made available for information purposes only. A summary of this decision is published in all EU languages in the Official Journal of the European Union.

Parts of this text have been edited to ensure that confidential information is not disclosed. Those parts are replaced by a non-confidential summary in square brackets or are shown as [...].



Brussels, 19.3.2025
C(2025) 3000 final

COMMISSION IMPLEMENTING DECISION

of 19.3.2025

**pursuant to Article 8(2) of Regulation (EU) 2022/1925 of the European Parliament and
of the Council on contestable and fair markets in the digital sector**

**Case DMA.100203 – Article 6(7) – Apple – iOS – SP – Features for Connected Physical
Devices**

(Only the English text is authentic)

COMMISSION IMPLEMENTING DECISION

of 19.3.2025

pursuant to Article 8(2) of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector

Case DMA.100203 – Article 6(7) – Apple – iOS – SP – Features for Connected Physical Devices

(Only the English text is authentic)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2022/1925 of the European Parliament and of the Council of 17 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act),¹ and in particular Article 8 thereof,

After consulting the Digital Markets Advisory Committee,

Whereas:

1. BACKGROUND TO THESE SPECIFICATION PROCEEDINGS

1.1. Introduction

- (1) On 5 September 2023, the Commission designated Apple Inc. together with all legal entities directly or indirectly controlled by Apple Inc. (hereinafter referred to as “Apple”) as a gatekeeper pursuant to Article 3(4) of Regulation (EU) 2022/1925 (“Designation Decision”)² for its core platform service (“CPS”) iOS, Apple’s operating system that powers Apple’s brand of smartphones: the iPhone. Following the designation of Apple’s iOS as a CPS, Apple had to comply with the obligations laid down in Articles 5, 6 and 7 of Regulation (EU) 2022/1925 by 7 March 2024.
- (2) Pursuant to Article 8(1) of Regulation (EU) 2022/1925, it is up to the gatekeeper to ensure and demonstrate compliance with its obligations, and the measures implemented by the gatekeeper shall be effective in achieving the objectives of the Regulation and of the relevant obligation. Regulation (EU) 2022/1925 empowers the Commission to enforce the gatekeeper’s compliance with the obligations set out in that Regulation.
- (3) In addition, pursuant to Article 8(2) of Regulation (EU) 2022/1925, the Commission may, on its own initiative or at the request of a gatekeeper, specify measures that the

¹ OJ L 265, 12.10.2022, pages 1-66.

² Decision C(2023) 6100 final. On 29 April 2024, the Commission adopted a decision amending the Designation Decision to include Apple’s operating system iPadOS as a core platform service which individually constitutes an important gateway for business users to reach end users (see Decision C(2024) 2500 final).

gatekeeper should implement to effectively comply with certain obligations. Article 6(7) of Regulation (EU) 2022/1925 is an obligation that is susceptible of being further specified.

1.2. Apple's approach towards compliance with Article 6(7) of Regulation (EU) 2022/1925

- (4) On 7 March 2024, Apple submitted its compliance report pursuant to Article 11 of Regulation (EU) 2022/1925 ("Apple's Compliance Report") to the Commission.³ In that report, Apple announced three measures it intended to take to comply with Article 6(7) of Regulation (EU) 2022/1925 in relation to Apple's iOS CPS.⁴ In the revised compliance report submitted by Apple on 1 November 2024, Apple stated that these measures have been introduced for the iOS CPS (and iPadOS CPS).⁵ Apple has introduced:
- (a) an engineering team focused on ensuring that Apple provides third parties with effective interoperability with newly released iPhone and iOS hardware and software features, at least to the extent required by Article 6(7) of Regulation (EU) 2022/1925;
 - (b) a new request form for eligible⁶ developers to request additional interoperability with hardware and software features built into the iPhone and Apple's iOS CPS ("Interoperability Request Portal"); and
 - (c) new capabilities for alternative browser engines to interoperate with iOS.
- (5) In Apple's Compliance Report, Apple explained that it had already put in place certain interoperability practices before the compliance date of Regulation (EU) 2022/1925 and irrespective of its obligations under that Regulation.⁷ In particular, Apple explained that it offers development tools to help developers write software and offer hardware that interoperates with iOS. Apple also explained that it operates a "Made for iPhone" licensing programme, which enables third parties to develop hardware accessories using Apple technologies, including technical specifications and resources needed to communicate with Apple devices. Furthermore, Apple recalled it implements numerous industry standards, including to connect the iPhone via Bluetooth or other short-range technology standards with third-party accessories, and standards for hardware functionality such as Wi-Fi and USB.

1.3. Interoperability requests concerning connected physical devices

- (6) Already before the launch of the Interoperability Request Portal by Apple and shortly thereafter, between January and March 2024, Apple received several requests for

³ Apple's Compliance Report.

⁴ Apple's Compliance Report, pages 21, 73-76.

⁵ Apple's revised Compliance Report submitted on 1 November 2024, pages 21, 73-79. For completeness, the Commission notes that in the latest compliance report, submitted by Apple on 7 March 2025, Apple describes, with respect to its compliance with Article 6(7) of Regulation (EU) 2022/1925, the same measures that it had described in previous versions of its compliance report.

⁶ To be eligible, the developer's Apple Developer Program membership must be in good standing and the developer must have entered into the current terms of the Apple Developer Program License Agreement, cf. Apple's revised Compliance Report submitted on 1 November 2024, page 76, Annex 15 to Section 2, paragraph 14.

⁷ Apple's Compliance Report, page 72.

effective interoperability under Article 6(7) of Regulation (EU) 2022/1925 with regard to connected physical devices.⁸

- (7) Connected physical devices include any physical object which incorporates a connectivity function allowing for the exchange of data, i.e. the transmission or reception of data, with another device over a wired or wireless transmission channel.⁹ This includes both physical objects that have already established connectivity with another device, as well as physical objects that themselves incorporate a connectivity function, but where such connectivity has not yet been established with another device.
- (8) The requests related to connected physical devices concern effective interoperability with, and access for the purpose of interoperability to, iOS features¹⁰ relating *inter alia* to notifications, the data connection to synchronize and transmit high data volumes, pairing of the connected physical device with the iOS device, and other aspects of establishing and maintaining connectivity.

1.4. Importance of effective interoperability with iOS for connected physical devices

- (9) Achieving effective interoperability under Article 6(7) of Regulation (EU) 2022/1925 is of paramount importance to ensure contestability of services and hardware offered to end users for which iOS acts as an important gateway. Apple's own services and hardware, including its connected physical devices, are integrated and connected with iOS. The integration creates an ecosystem that provides end users with a seamless experience across Apple devices, but also has the effect of locking end users into that ecosystem.¹¹
- (10) Access under equal conditions to iOS features allows third-party providers of connected physical devices to compete with Apple's own connected physical devices on an equal footing and to develop and to offer new innovative connected physical devices which rely on access to iOS to reach end users. Lowering barriers to entry and expansion by providing access to iOS to third-party providers of connected physical devices will increase the incentives and the ability for such third-party providers to innovate and improve their products available through and on iOS, ultimately increasing end user choice for connected physical devices.¹²
- (11) Indeed, consumers will be able to freely choose the connected physical devices that best suit their personal preferences, independently of considerations on whether some operating system features may not work with those devices. Consumers will also be able to switch between different operating systems without risking losing the benefits of interoperability or functionalities of connected physical devices they already own.
- (12) The Commission also notes that interoperability with regard to connected physical devices is of substantial economic importance. Many requests received by Apple

⁸ See Section 4 of this Decision.

⁹ This includes payment cards and accessories, such as wearables, including passive wearables, for instance rings, with a Near-Field Communication chip. It also includes vehicles which incorporate a connectivity function. It suffices that the physical object can either transmit or receive data.

¹⁰ iOS features refer to hardware and software features accessed or controlled via iOS within the meaning of Article 6(7), first subparagraph first sentence, of Regulation (EU) 2022/1925 and iOS, hardware or software features within the meaning of Article 6(7), first subparagraph, second sentence of that Regulation.

¹¹ See, for example, Commission Decision of 29.04.2024, C(2024) 2500, recitals 39-43.

¹² See also Section 3.2 of this Decision.

pursuant to Article 6(7) of Regulation (EU) 2022/1925 concern interoperability for connected physical devices, such as wearables. According to publicly available forecasts, the global wearable technology market, which is only a subsegment of connected physical devices, was valued at USD 120.54 billion in 2023 and is projected to grow from USD 157.94 billion in 2024 to USD 1 415.26 billion by 2032, with an annual growth rate of 31.5% during the forecast period between 2024 and 2032.¹³ Apple estimates that most iOS devices (i.e. iPhones) do – at one point – connect to a physical device in the EU.¹⁴

1.5. Use of specification proceedings

- (13) While the obligation to achieve effective interoperability is clearly set out in Article 6(7) of Regulation (EU) 2022/1925, gatekeepers may need guidance as to how to implement it in relation to specific features of their designated operating systems. Such guidance may include aspects such as the exact interoperability solutions in relation to specific features, aspects of their technical implementation, and the modalities of access to be provided to third parties.
- (14) Article 8 of Regulation (EU) 2022/1925 sets out that the Commission, on its own initiative or at the request of a gatekeeper, can initiate proceedings to specify the measures that the gatekeeper is to implement in order to effectively comply with a specific obligation in Article 6 or 7 of that Regulation.
- (15) Recital 65 of Regulation (EU) 2022/1925 states that the Commission, following a dialogue with the gatekeeper concerned and after enabling third parties to make comments, may decide to further specify some of the measures that the gatekeeper concerned should adopt in order to effectively comply with obligations that are susceptible of being further specified or, in the event of circumvention, with all obligations.
- (16) Pursuant to Article 8(7) of Regulation (EU) 2022/1925, in specifying the measures that the gatekeeper concerned is to implement in order to effectively comply with its obligations, the Commission shall ensure that the measures are effective in achieving the objectives of that Regulation and the relevant obligation and proportionate in the specific circumstances of the gatekeeper and the relevant service.
- (17) The current proceedings focus on interoperability solutions for connected physical devices connected to iOS devices. These solutions were subject to various discussions between Apple and the Commission in the context of the requests made by third parties via the Interoperability Request Portal or outside this portal (see Section 4 of this Decision). While the measures in this Decision are informed by these requests, the Commission notes that a request in Apple's Interoperability Request Portal is not a pre-requisite for Commission's action under Article 8(2) of Regulation (EU) 2022/1925.
- (18) For the iOS features subject to this Decision, the Commission is concerned that effective interoperability within the meaning of Article 6(7) of Regulation (EU) 2022/1925 does not yet exist on iOS. These concerns are borne out in requests made by third parties via Apple's Interoperability Request Portal and submissions during the administrative proceedings and the public consultation. They are further borne

¹³ See <https://www.fortunebusinessinsights.com/wearable-technology-market-106000>, accessed on 27 August 2024.

¹⁴ Apple's reply to RFI 3 of 7 October 2024, question 55.

out by Apple's submissions outlining possible interoperability solutions and its proposed implementation deadlines.

- (19) Therefore, to swiftly provide effective interoperability solutions to the market, the Commission considers it appropriate to specify the measures that Apple should adopt to effectively comply with Article 6(7) of Regulation (EU) 2022/1925 with respect to connected physical devices in relation to Apple's operating system iOS in the European Union. To the extent relevant and applicable, such specifications might also provide useful indications regarding the measures that Apple should apply to allow for interoperability of connected physical devices in relation to Apple's other designated operating systems.
- (20) These proceedings are without prejudice to the measures specified in the decision of 19 March 2025 in the parallel specification proceedings on Process (DMA.100204). In case of conflict, the measures in the present Decision shall prevail.

2. PROCEDURE

2.1. Legal framework for specification proceedings

- (21) To specify the measures pursuant to Article 8(2) of Regulation (EU) 2022/1925, the Commission shall adopt an implementing act. This implementing act shall be adopted within six months from the opening of the proceedings pursuant to Article 20 of Regulation (EU) 2022/1925. Before adopting such an implementing act, the Commission shall communicate to the gatekeeper its preliminary findings, including the measures it is considering taking, within three months.
- (22) Pursuant to Article 8(6) of Regulation (EU) 2022/1925, to effectively enable interested third parties to provide comments, the Commission shall, when communicating its preliminary findings to the gatekeeper or as soon as possible thereafter, publish a non-confidential summary of the case and the measures that it is considering taking or that it considers the gatekeeper concerned should take. The Commission shall specify a reasonable timeframe within which such comments are to be provided.
- (23) Pursuant to Article 8(9) of Regulation (EU) 2022/1925, the Commission may, upon request or on its own initiative, decide to reopen specification proceedings where (i) there has been a material change in any of the facts on which the decision was based, (ii) the decision was based on incomplete, incorrect or misleading information, or (iii) the measures as specified in the decision are not effective.

2.2. Chronology of the current proceedings

- (24) Between June 2023 and September 2024, the Commission and Apple held numerous meetings, of which more than ten focused on Apple's compliance with Article 6(7) of Regulation (EU) 2022/1925. On 18 January 2024, during a meeting with Apple, the Commission and Apple discussed third parties' requests for interoperability regarding connected physical devices. The Commission sent to Apple requests for information regarding these interoperability requests enquiring whether Apple had provided effective interoperability with the requested iOS features on 19 February 2024, and further on 12 March 2024 and 2 April 2024.
- (25) On 3 September 2024, the Commission informed Apple of its intention to assist Apple in its compliance efforts in relation to certain iOS features for connected

physical devices and to its general interoperability request process through opening of specification proceedings pursuant to Article 8(2) of Regulation (EU) 2022/1925.

- (26) On 19 September 2024, the Commission adopted a decision opening proceedings pursuant to Article 20(1) of Regulation (EU) 2022/1925 with a view to adopting a decision pursuant to Article 8(2) of that Regulation specifying the measures that Apple has to implement regarding its operating system iOS in order to effectively comply with Article 6(7) of that Regulation for certain iOS features for connected physical devices (“Decision opening specification proceedings”).¹⁵
- (27) On 25 September 2024, the Commission held a state of play meeting with Apple in which it outlined to Apple the preliminary scope of the specification proceedings and a proposal for a constructive engagement centred around technical meetings, in line with the spirit of the regulatory dialogue and Article 8 of Regulation (EU) 2022/1925.
- (28) The Commission held a total of six technical meetings with Apple between 3 October 2024 and 7 November 2024, together covering all of the iOS features in the scope of these proceedings.¹⁶
- (29) In the context of these proceedings the Commission sent to Apple 12 requests for information (“RFIs”), as well as an RFI by decision on 26 September 2024 requesting internal documents from Apple.¹⁷
- (30) On 21 November 2024, prior to the adoption of the preliminary findings, the Commission held with Apple a courtesy state-of-play conference call during which the Commission outlined the scope of the preliminary findings.
- (31) In a conference call with Apple on 17 December 2024, following further submissions by Apple, the Commission and Apple further discussed technical aspects related to the interoperability of Apple’s AirPlay and AirDrop.¹⁸
- (32) On 18 December 2024, the Commission communicated its preliminary findings to Apple pursuant to Articles 8(5) and 34(1) of Regulation (EU) 2022/1925 (“Preliminary Findings”), providing Apple with the opportunity to comment on its findings and the proposed measures by 17 January 2025.
- (33) On the day of the adoption of the Preliminary Findings, Apple requested access to the Commission’s file pursuant to Articles 8(1), 8(2) and 8(3) of the Commission Implementing Regulation (EU) 2023/814. On that same day and in reply to Apple’s request, the Commission provided Apple with all documents used in the Preliminary Findings pursuant to Article 8(2) of the Commission Implementing Regulation (EU) 2023/814. On the day following Apple’s request, i.e. 19 December 2024, the Commission afforded Apple’s external legal counsel access to the case file in a data room pursuant to Article 8(3) of the Commission Implementing Regulation (EU) 2023/814. Access to the data room was provided on 19 and 20 December 2024 and continued from 6 until 8 January 2025. Apple did not request an extension of the data room access. In the context of the data room, Apple’s external legal counsel prepared

¹⁵ Decision C(2024) 6663 final.

¹⁶ Technical Meetings took place on 3 October 2024, 9 October 2024, 14 October 2024, 18 October 2024, 24 October 2024, and 7 November 2024.

¹⁷ Decision C(2024) 6879 final of 26 September 2024, amended on 14 October 2024 (Commission Decision C(2024) 7318 final).

¹⁸ Email from Apple to the Commission of 12 December 2024 [on AirPlay and AirDrop].

a [...] data room report. The [...] data room report was shared with Apple on 8 January 2025.¹⁹

- (34) On 18 December 2024, and in line with Article 8(6) of Regulation (EU) 2022/1925, the Commission published a non-confidential summary of the case and the proposed measures to enable interested third parties to provide their comments on the proposed measures, including their technical feasibility.
- (35) The public consultation was open until 9 January 2025, with the Commission granting extensions until 15 January 2025 upon request. The Commission received 63 contributions from third parties, end users and other interested third parties. All submissions were shared with Apple on a rolling basis, as agreed with Apple's external legal counsel.²⁰
- (36) On 10 January 2025, Apple requested an extension to respond to the Preliminary Findings. On 13 January 2025, the Commission granted an extension until 20 January 2025, thereby granting Apple a total of one calendar month or 20 working days to submit its observations.
- (37) On 20 January 2025, Apple provided its response to the Preliminary Findings ("Apple's reply to the Preliminary Findings").²¹
- (38) On 23 January 2025, Apple submitted a mark-up of the measures described in the Annex of the Preliminary Findings in relation to the specific iOS features ("Apple's mark-up of the Commission's proposed measures of 23 January").²²
- (39) On 24 and 29 January 2025, the Commission held meetings with Apple to discuss Apple's feedback on the measures. On 27 and 28 January 2025, the Commission held tripartite meetings with Apple and [third-party developer] and [third-party developer] respectively. The meetings were followed by an additional submission by [third-party developer]²³ and additional conference calls²⁴ to clarify various aspects of Apple's concerns.
- (40) On 31 January 2025, Apple sent an additional mark-up of the Commission's general measures ("Apple's mark-up of the Commission's proposed measures of 31 January 2025").²⁵
- (41) By way of courtesy, the Commission shared the proposed final measures ("Draft Final Measures") with Apple on 7 February 2025, granting Apple until 14 February 2025 to submit its observations and offering a meeting to provide any clarification.²⁶
- (42) On 11 and 12 February 2025, upon Apple's request, two meetings were held where Apple had the opportunity to comment on the Draft Final Measures. Following up on this, Apple provided further written comments on the Draft Final Measures in writing

¹⁹ Data Room Report [...].

²⁰ The Commission sent third parties' contributions to Apple via email on 20 December 2024, 3 January 2025, 8 January 2025, 13 January 2025, and 16 January 2025.

²¹ Apple's reply to the Preliminary Findings.

²² Apple's mark-up of the Commission's proposed measures of 23 January.

²³ [Third-party developer]'s submission of 29 January 2025.

²⁴ Two meetings with Apple on 29 January 2025 and 3 February 2025, one meeting with [third-party developer] on 3 February 2025 and meeting with [third-party developer] on 3 February 2025. The minutes of these meetings were provided to Apple on 5 February 2025.

²⁵ Apple's mark-up of the Commission's proposed measures of 31 January 2025.

²⁶ Email from [the Commission to Apple of 7 February 2025 on the draft final measures].

on 13 and 17 February 2025.²⁷ On 21 February 2025, Apple sent another email summarising its position.²⁸

- (43) On 15 March 2025, five calendar days or four working days before the legal deadline for the final decision in the case, Apple submitted a letter to the Commission, in which it set out its concern that the specification proceedings impact Apple's intellectual property rights ("IPRs"). [...] ²⁹

2.3. Commission's engagement with Apple

- (44) Against the background of the regulatory dialogue with Apple concerning the implementation of Apple's obligations under Article 6(7) of Regulation (EU) 2022/1925, which has been ongoing since the designation of Apple's operating system iOS, the Commission conducted the specification proceedings in a diligent and transparent manner, taking account of the framework of Regulation (EU) 2022/1925. As described in Section 2.2 of this Decision, the Commission actively engaged with Apple throughout the proceedings.
- (45) *First*, following a number of meetings on the issues within the scope of these proceedings, Apple was made aware of the upcoming formal opening of the proceedings more than two weeks ahead of the adoption of the Decision opening specification proceedings. To make the process as constructive as possible, the Commission planned and held six technical meetings prior to adopting Preliminary Findings, for which the Commission agreed with Apple a clear and detailed timetable of engagement while ensuring sufficient time to discuss each of the aspects within the scope of the proceedings. For most technical meetings, which lasted approximately four hours each, the Commission scheduled fallback meetings on the following day with Apple, to ensure sufficient time for the discussions. Apple never expressed an interest to use this additional time to extend any of the discussions, even when explicitly queried. During these technical meetings Apple presented slide decks explaining its view of the features and effective interoperability.
- (46) *Second*, the Commission issued 10 RFIs to Apple to inform its views and assessment ahead of the issuance of the Preliminary Findings. Whilst acknowledging the short timelines imposed by the Regulation (EU) 2022/1925, the Commission set appropriate deadlines in its RFIs. All of Apple's extension requests to reply to an RFI were accommodated (with one exception, where only a partial extension was granted – 12 hours less than requested).
- (47) *Third*, the Commission engaged extensively with Apple on Apple's compliance with the RFI by decision of 26 September 2024, which required Apple to produce internal documents from a limited number of custodians subject to keywords, as well as certain categories of documents based on a description. The deadline to produce the documents was 25 October 2024, i.e. one calendar month. On 2 October 2024, Apple submitted a reasoned request asking to adjust the search terms, custodians and to extend the deadline to comply with the request. Following Apple's reasoned request as well as meetings with Apple, the Commission amended the internal document request to adjust (i.e. decrease) the number of keywords and custodians and extended the deadline for certain categories of documents to 10 November 2024.

²⁷ Agreed minutes of meetings with Apple on 11 and 12 February 2025.

²⁸ Email from Apple to the Commission of 21 February 2025 [on the specification proceedings].

²⁹ Letter from Apple dated 14 March 2025 (received on 15 March 2025).

- (48) Apple produced the first set of responsive documents on 26 October 2024 and continued to submit several productions of responsive documents. On 11 November 2024, Apple sent an email to the Commission explaining that technical issues with the software used in the document collection led to a delay for the collection of certain categories of documents.³⁰ Apple continued to produce responsive documents until 22 November 2024, on which day it sent a statement on material completion to the Commission. Apple submitted further sets of responsive documents to the Commission on 24 November 2024, 6 January 2025, 8 February 2025, and 17 March 2025, which, according to Apple, were identified during a final check or were missing from previous productions due to technical issues.
- (49) On 21 January 2025, the Commission sent a letter to Apple concerning the legal privilege claims in the produced responsive documents, setting out issues concerning (i) the number of documents fully withheld due to their allegedly privileged nature, (ii) the completeness of the privilege log, and (iii) other matters relating to the privilege log, such as categorisation of claims and submission of the audit log. Apple replied to this letter on 29 January 2025 and sent a revised version of the accompanying report.
- (50) *Fourth*, the Commission reviewed at least 18 submissions made by Apple throughout these proceedings.³¹ All these submissions and discussions informed the Commission's assessment in these proceedings and the measures described below.
- (51) *Fifth*, as described in Section 2.2 of this Decision, the Commission continued the engagement with Apple after the adoption of the Preliminary Findings. In particular, the Commission: (i) reviewed mark-ups of the draft measures, which Apple sent to the Commission after the deadline to reply to the Preliminary Findings; (ii) held meetings with Apple to discuss Apple's feedback on the measures; and (iii) moderated tripartite meetings between Apple and developers who had requested interoperability. These meetings were followed by multiple other exchanges of views via email and conference calls.
- (52) *Sixth*, and for the sake of completeness, the Commission sent all submissions of third parties to the public consultation to Apple on a rolling basis, as well as all minutes of meetings with third parties that took place after the adoption of the Preliminary Findings, irrespective of whether these documents are used in this Decision.³²
- (53) *Seventh*, and in the spirit of good cooperation,³³ the Commission sent the Draft Final Measures to Apple on 7 February 2025, granting Apple an additional opportunity to comment on the Commission's Draft Final Measures. Following this, the Commission engaged further with Apple on its views and comments on the Draft Final Measures.
- (54) As part of the intense regulatory dialogue between Apple and the Commission in the context of these proceedings as described in Sections 2.2 and 2.3 of this Decision,

³⁰ Apple first alerted the Commission of possible technical issues in its reasoned submission on 2 October 2024 and provided updates in calls on 24 October and 6 November 2024.

³¹ Submissions of 15 October 2024, 24 October 2024, 6 November 2024, 7 November 2024, 14 November 2024, 16 November 2024, 12 December 2024, 18 December, 28 January 2025, 29 January 2025, 2 February 2025, 3 February 2025, 13 February 2025, and 17 February 2025.

³² Minutes of meetings of 9, 13, and 17 January and 3 February 2025. All minutes were shared with Apple by email on 5 February 2025.

³³ [...]

Apple outlined a number of preliminary ideas for potential interoperability solutions concerning the features covered by these proceedings. The Commission notes that most of these proposals were brief and vague, consisting of a few bullet points, slides or oral remarks during meetings and conference calls with the Commission, and often came at a late stage of the process. Nevertheless, the Commission assessed these ideas and used this assessment, where considered appropriate, as input for designing the measures in the Annex to this Decision.³⁴ Pursuant to the measures for all features specified in the Annex to this Decision, Apple has one month as of the date of notification of this Decision to provide details on its implementation plans.³⁵ These will be reviewed and monitored by the Commission following the adoption of the Decision in the context of the Commission's duties pursuant to Article 26(1) of Regulation (EU) 2022/1925. Hence, the assessment of the actual compliance by Apple does not form part of the specification proceedings but shall be reviewed and monitored by the Commission following the adoption of the decision pursuant to Articles 8(2) and 26(1) of Regulation (EU) 2022/1925.

- (55) In light of the above, and taking into account the extent of the Commission's engagement with Apple as set out in this Section and Section 2.2 of this Decision, the Commission considers that it discharged its duties under Article 41 of the Charter (right to good administration). Contrary to Apple's claims,³⁶ the Commission duly considered Apple's submissions on the principle of proportionality, Apple's fundamental rights and Apple's intellectual property rights ("IPRs") as set out in Section 6 of this Decision.³⁷ [...] ³⁸ [...] ³⁹ Apple's claims that the Commission did not reply to all its submissions and arguments prior to the adoption of the Preliminary Findings disregard that the object of the Preliminary Findings is precisely to give Apple the opportunity to be heard on the Commission's findings and the measures the Commission may specify as a result: should Apple consider that its prior submissions have not been duly taken into account, the reply to the Preliminary Findings allows Apple to argue accordingly, as it has. Moreover, it is established case law that, even in adversarial procedures which would result in a fine, the duty to state reasons does not require the Commission to reply to every individual submission and argument raised by the undertaking during the administrative procedure. In its reply to the Preliminary Findings, Apple was able to respond to

³⁴ For instance, this is the case for the high-bandwidth peer-to-peer Wi-Fi connection features (see Section 5.4 of this Decision), where the Commission assessed and even specified the interoperability solution put forward by Apple, namely Wi-Fi Aware (instead of AWDL). Similarly, for the proximity-triggered pairing feature, the Commission assessed and took into account Apple's proposed solution (see Section 5.5 of this Decision).

³⁵ Paragraph 101(l) of the Annex to this Decision.

³⁶ Apple's reply to the Preliminary Findings, Section VIII.

³⁷ Apple's reply to the Preliminary Findings, paragraph 375.

³⁸ Apple's reply to the Preliminary Findings, paragraphs 376.b and 377. Apple has not duly justified its integrity concerns regarding NFC Reader/Writer mode, see Section 5.11.6.3 of this Decision. The Commission informed Apple of the scope of the NFC Reader/Writer mode, see footnote 611 of this Decision.

³⁹ Apple's reply to the Preliminary Findings, paragraph 376.c. Apple's claims about integrity concerns regarding automatic Wi-Fi connection were unsubstantiated prior to the adoption of the Preliminary Findings. In fact, only in Apple's mark-up of the Commission's proposed measures of 23 January, did Apple even propose a mitigating measure, although again in an unsubstantiated way (see Section 4.7.7 of this Decision for details). In particular, Apple's submission of 7 November 2024 and the cited slide deck presented on 18 October 2024, do not mention the automatic Wi-Fi connection or discuss any integrity, privacy or security concerns relevant to that feature.

each of the reasons put forward by the Commission justifying the measures it intended to take.⁴⁰

3. INTEROPERABILITY OBLIGATION PURSUANT TO ARTICLE 6(7) OF REGULATION (EU) 2022/1925

- (56) Pursuant to Article 6(7) of Regulation (EU) 2022/1925, gatekeepers shall:
- (a) allow providers of services and providers of hardware, free of charge, effective interoperability with, and access for the purposes of interoperability to, the same hardware and software features accessed or controlled via the operating system or virtual assistant listed in the designation decision pursuant to Article 3(9) of Regulation (EU) 2022/1925 as are available to services or hardware provided by the gatekeeper; furthermore, the gatekeeper shall allow third parties and alternative providers of services provided together with, or in support of, CPSs, free of charge, effective interoperability with, and access for the purposes of interoperability to, the same operating system, hardware or software features, regardless of whether those features are part of the operating system, as are available to, or used by, that gatekeeper when providing such services; and
 - (b) not be prevented from taking strictly necessary and proportionate measures to ensure that interoperability does not compromise the integrity of the operating system, virtual assistant, hardware or software features provided by the gatekeeper, provided that such measures are duly justified by the gatekeeper.
- (57) Article 2(29) of Regulation (EU) 2022/1925 defines interoperability as the ability to exchange information and mutually use the information which has been exchanged through interfaces or other solutions, so that all elements of hardware or software work with other hardware and software and with users in all the ways in which they are intended to function.
- (58) Pursuant to Article 8(1) of Regulation (EU) 2022/1925, the gatekeeper shall ensure that the implementation of measures implemented to ensure compliance with Article 6(7) of that Regulation complies with applicable law, in particular Regulation (EU) 2016/679, Directive 2002/58/EC, legislation on cybersecurity, consumer protection, product safety, as well as with the accessibility requirements.
- (59) While the measures that gatekeepers may introduce in relation to the interoperability solutions are limited to integrity measures, this does not exclude that gatekeepers may apply measures enabling end users to effectively protect security in relation to third-party software applications, pursuant to Article 6(4) of Regulation (EU) 2022/1925. Furthermore, software application store providers (including a software application store in relation to which a gatekeeper may have been designated, subject to Regulation (EU) 2022/1925 and in particular Article 6(12) of that Regulation) may introduce safeguards⁴¹ to prevent abuse by malicious actors, protect the security and privacy of end users, and comply with applicable law (in particular Regulation (EU)

⁴⁰ See in that regard, judgment of 9 April 2019, *Qualcomm v Commission*, T-371/17, EU:T:2019:232, paragraphs 70-71 and case law cited. See also judgment of 24 May 2023, *Meta v Commission*, T-451/20, EU:T:2023:276, paragraph 160.

⁴¹ Such safeguards should not undermine effective interoperability with features as prescribed in Article 6(7) of Regulation (EU) 2022/1925 and implementing acts specifying measures that a gatekeeper should implement to effectively comply with the obligation in that Article.

2022/2065,⁴² Regulation (EU) 2016/679, Directive 2002/58/EC, legislation on cyber security, consumer protection, product safety, as well as with the accessibility requirements) for apps distributed on their stores.

3.1. Scope of Article 6(7) of Regulation (EU) 2022/1925 – effective interoperability

3.1.1. Interoperability with the same features as available to the gatekeeper Apple and under equal conditions

- (60) Pursuant to Article 6(7) of Regulation (EU) 2022/1925, effective interoperability and access for the purposes of interoperability should be granted with the same features as are available or used by the gatekeeper’s services or hardware.
- (61) The use of the adjective “*same*” implies that the very same feature – not a similar one – needs to be made accessible to third parties. Recitals 55 and 57 of Regulation (EU) 2022/1925 clarify that the interoperability solution should be equally effective to the solution available to the gatekeeper and should be made available under equal conditions. Equal effectiveness and equality of conditions are assessed by comparison to how the gatekeeper implements interoperability and access to hardware and software features for its own services and hardware. It includes aspects both user-facing and non-user-facing, such as the end user journey, ease of use, device and software set-up, data transmission speed, and energy consumption. Indeed, these may be critical properties of the feature itself.
- (62) Apple argued that Article 6(7) of Regulation (EU) 2022/1925 simply requires Apple to allow for interoperability which is effective, i.e. putting third parties in a position to offer an “*alternative solution*,” but does not mandate that interoperability must be “*equally effective*” to the solution available to Apple or be provided “*under equal conditions*.”⁴³
- (63) The Commission notes that Apple’s position is contradicted by the language and aim of Article 6(7) of Regulation (EU) 2022/1925 and its respective recitals. By referring to “*the same features*” in Article 6(7) of Regulation (EU) 2022/1925 and the need for “*equally effective interoperability*” in recital 55 of that Regulation, the EU legislator made a clear distinction. On the one hand, the feature – the “*what*” of the interoperability – needs to be the same as the feature available to the gatekeeper’s services and hardware. On the other hand, the actual interoperability solution – the “*how*” of the interoperability – needs to be “*equally effective*” to the solution available to the gatekeeper and be provided “*under equal conditions*,” without necessarily being exactly the same solution. By mandating an equally effective interoperability solution, the legislator acknowledged that the implementation of interoperability does not always need to (and potentially cannot always) be the same for the gatekeeper and third parties, but interoperability must be granted to the same feature under equal conditions.
- (64) Providing interoperability with the same feature allows third parties to offer their services and hardware and innovate on an equal footing with the gatekeeper. Access to a partial, degraded or barren feature would not create a level playing field required

⁴² Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 27.10.2022, p. 1-102.

⁴³ Apple’s reply to the Preliminary Findings, Sections IV.A., IV.C. and V.C.

under Article 6(7) of Regulation (EU) 2022/1925 and is therefore liable to undermine the goals of contestability and fairness of that Regulation.

- (65) The interpretation of Article 6(7) of Regulation (EU) 2022/1925 proposed by Apple is at odds with the clear language of that provision, which refers, as explained, to the “same” features. Apple’s interpretation would also be contrary to the legislator’s aim to ensure legal certainty and to facilitate *ex ante* compliance so that business and end users can benefit from Regulation (EU) 2022/1925 without delay.⁴⁴ The legislator achieved this goal by requiring interoperability with the same feature in a way that is equally effective as the solution available to the gatekeeper independently of the feature and third party. It is entirely unclear what level of interoperability would be required under the legal tests proposed by Apple: [Apple explains legal tests taking into account several considerations, such as technical requirements, tools for alternative solutions, and the necessary level of interoperability.]⁴⁵ [...] ⁴⁶ [...] ⁴⁷ [...] ⁴⁸ [...] ⁴⁹
- (66) Common to Apple’s proposed legal standards is the need to assess why third parties are currently unable to provide a “competitive offering” or an “alternative solution.” Such an assessment, which would require an individual examination of the specific circumstances of each third party, is not required by Article 6(7) of Regulation (EU) 2022/1925. Such an assessment would introduce the requirement to investigate on a case-by-case basis the effects on competition of a gatekeeper’s given conduct, which the legislator explicitly rejected.⁵⁰ Moreover, this would undermine effective and timely compliance, also affecting Apple’s general obligation to demonstrate compliance under Article 8(1) of Regulation (EU) 2022/1925.
- (67) Apple’s statements regarding specific features further underline how its approach is in contradiction with the wording and the aim of Article 6(7) of Regulation (EU) 2022/1925. For example, for iOS notifications, Apple claims that the Commission must conduct “a rigorous assessment of the [...] importance of the notifications functionalities and their impact on contestability,”⁵¹ even for the basic functionality that end users can reply to notifications on third-party smartwatches just like on the Apple Watch. Such an assessment of impact or effects is not provided for in Regulation (EU) 2022/1925, nor is the scope of Article 6(7) of that Regulation limited to features of “importance.” In another instance, for the NFC controller in Reader/Writer Mode, Apple argued that it already provides “the tools necessary” for interoperability⁵² based on the fact that one single developer was able to develop a “technical workaround” requiring significant engineering work and delaying its

⁴⁴ Recital 5 of Regulation (EU) 2022/1925. The legislator adopted that regulation to aid the shortcomings that antitrust “enforcement occurs *ex post* and requires an extensive investigation of often very complex facts on a case-by-case basis.”

⁴⁵ Apple’s reply to the Preliminary Findings, paragraph 55.

⁴⁶ Apple’s reply to the Preliminary Findings, paragraph 6, second bullet.

⁴⁷ Apple’s reply to the Preliminary Findings, paragraph 53.

⁴⁸ Apple’s reply to the Preliminary Findings, paragraph 57.

⁴⁹ Apple’s reply to the Preliminary Findings, paragraphs 55 and 20.

⁵⁰ Recital 11 of Regulation (EU) 2022/1925: “This Regulation pursues an objective that is complementary to, but different from that of protecting undistorted competition on any given market, as defined in competition-law terms, which is to ensure that markets where gatekeepers are present are and remain contestable and fair, independently from the actual, potential or presumed effects of the conduct of a given gatekeeper covered by this Regulation on competition on a given market.”

⁵¹ Apple’s reply to the Preliminary Findings, paragraph 127.

⁵² Apple’s reply to the Preliminary Findings, paragraph 365.

product launch by several years.⁵³ Again, the Commission reiterates that Article 6(7) of Regulation (EU) 2022/1925 does not provide for an assessment of whether making available some capability of a feature could, under certain circumstances or for certain third parties, be sufficient to safeguard contestability, but instead mandates effective interoperability with the same feature as available to Apple's services or hardware.

3.1.2. *Features and functionalities*

- (68) The scope of a specific feature must be assessed in light of the goal of Article 6(7) of Regulation (EU) 2022/1925 to ensure that capabilities controlled by the operating system are not reserved by the gatekeeper for its own services or hardware, which would be contrary to the clear language and objective of Article 6(7) of that Regulation. Features within the meaning of Article 6(7) of Regulation (EU) 2022/1925 include capabilities that the operating system makes available to the gatekeeper's services or hardware. Such capabilities encompass technical functionalities of the device on which the operating system runs, such as near-field-communication technology, secure elements and processors, authentication mechanisms and the software used to operate those technologies.⁵⁴
- (69) Therefore, a feature consists of one or more functionalities.⁵⁵ A functionality alone, or in combination with other functionalities, may be necessary to enable access to a feature. Therefore, denying or undermining access to a functionality may be tantamount to denying or undermining access to a feature. For example, the iOS notifications feature includes a functionality to read notifications and a functionality to reply to them. Undermining access to any of them would undermine access to the iOS notifications feature.
- (70) Apple disputes that a feature can consist of several functionalities and argues that there is no obligation to provide access to the same functionalities as available to Apple.⁵⁶ The Commission rejects this interpretation, as it would allow gatekeepers, by withholding access to a functionality, to withhold access to a feature of the operating system and preserve that feature exclusively for its own services or hardware. Whenever a feature consists of several functionalities, effective interoperability with that feature requires interoperability with all of those functionalities.⁵⁷ Providing access to only some functionalities of a feature would not amount to effective interoperability with that same feature and would be contrary to the objective of Article 6(7) of Regulation (EU) 2022/1925 to create a level playing field.

⁵³ Agreed minutes of meeting with [third-party developer] of 29 October 2024, paragraphs 3-7.

⁵⁴ Recital 56 of Regulation (EU) 2022/1925.

⁵⁵ A functionality of a feature may be a feature in its own right. This is similar to how intermediate products in a manufacturing supply chain are produced from other intermediate products in earlier steps of the manufacturing process, but also serve as inputs for subsequent steps. For operating systems, these layered components are collectively called "software stack". Third-party applications are built using components at different levels of the software stack, with each component providing some capabilities to applications.

⁵⁶ Apple's reply to the Preliminary Findings, Section V.D.

⁵⁷ In the Preliminary Findings, the Commission used the expression "feature functionality" as a shorthand for "functionality of the feature". In this decision, the expression has been replaced with "functionality of the feature" or just "functionality" when clear from the context, but the meaning has not changed.

3.1.3. *Future updates and new functionalities*

- (71) Article 6(7) of Regulation (EU) 2022/1925 aims at ensuring that third-party providers of services and hardware relying on an operating system to access their users are able to provide their services and hardware on a level playing field with the gatekeeper's services and hardware, insofar as access to the operating system is required.⁵⁸ A level playing field only exists if third-party providers of connected physical devices or related services obtain effective access to any updates, including new functionalities, at the same time as the gatekeeper and under equal conditions. In practice, this means that third parties need to be able to test any of such planned updates or new functionalities and obtain access to them once they are available to the gatekeeper's own services or hardware.
- (72) Apple argues that it does not need to allow third parties with interoperability for future updates, including new functionalities, of the features controlled or accessed via iOS at the same time as they are available to Apple. According to Apple, such an obligation is not within the scope of Article 6(7) of Regulation (EU) 2022/1925 and would limit Apple's incentives to innovate, increase the development cost of new features, reduce Apple's competitive advantage and allow third parties to free ride on Apple's innovation.⁵⁹
- (73) In this respect the Commission notes that Article 6(7) of Regulation (EU) 2022/1925 sets out that if a feature is available to or used by a gatekeeper, it needs to be made available and fully interoperable for third parties. Recital 65 of that Regulation further stipulates that a gatekeeper should ensure compliance with Regulation (EU) 2022/1925 by design and deploy a proactive approach to compliance. Especially for new functionalities of features which have already been made interoperable, it is unclear why a gatekeeper would not be able to design and implement these functionalities as interoperable from the start. If such updates were not made interoperable, the effective interoperability that was previously granted would regress.
- (74) The Commission also notes that contrary to Apple's claims,⁶⁰ providing interoperability with new features and functionalities when they become available to the gatekeeper does not deprive the gatekeeper of its incentives to innovate or of its competitive advantage. As regards Apple, this is clear from the following observations.
- (a) *First*, any development or improvement of iOS features improves in the first place iOS itself, and therefore its attractiveness to end users. As such, these development efforts benefit first and foremost Apple as the exclusive provider of iPhones – the only devices that can run iOS. Article 6(7) of Regulation (EU) 2022/1925 does not take this advantage away from Apple.
- (b) *Second*, even with full interoperability, Apple continues to enjoy an intrinsic advantage in the development of services and hardware accessing iOS features. As the developer of iOS, only Apple decides which iOS features are being prioritized, planned and developed. Apple can use this privileged position for the development of its services and hardware that make use of the respective

⁵⁸ Recital 55 of Regulation (EU) 2022/1925.

⁵⁹ Apple's reply to the Preliminary Findings, Section V.F.d.

⁶⁰ Apple's reply to the Preliminary Findings, paragraph 101.

iOS features. Apple can thus already design its products to integrate with those new iOS features in parallel – and will often design new iOS features precisely to support innovations to its products – ahead of any third party. Third parties will have access to the iOS feature at the same time (i.e. in the same iOS release) as Apple starts using the feature for its services and hardware, but the third parties then still need to go through implementing the new iOS feature for their own services and hardware, while Apple can already fully use it from day one after the iOS release. This Decision does not require Apple to disclose its internal development plans and pipeline to third parties. However, once a (new or updated) feature becomes available to Apple’s services or hardware, Apple needs to make the feature available to third parties. A further delay would not be reconcilable with the obligation to grant access “*under equal conditions*” and afford Apple an even greater first-mover advantage, making it very difficult or impossible for third parties to effectively compete with Apple on a level playing field.⁶¹ On the contrary, if Apple’s argumentation were to be validated it would leave it entirely to Apple’s discretion as of the time it would need to provide interoperability for new functionalities.

- (c) *Third*, Apple fails to take into account the overall incentives and opportunities for innovation that interoperability creates, both for Apple and for third parties. As set out in Section 3.2 of this Decision, a more open ecosystem does not preclude innovation of Apple’s products or features subject to this Decision. Furthermore, access to features under equal conditions fosters contestability and fairness for third parties dependent on Apple’s operating system and indirectly increases Apple’s incentives to bring innovation within iOS.

3.1.4. *Eligibility of beneficiaries, apps and use cases*

- (75) Article 6(7) of Regulation (EU) 2022/1925 does not provide for any limitations as to the beneficiaries, apps, products, and use cases for interoperability with iOS features, insofar as this feature is available to, or used by, the gatekeeper. If a business user or end user is eligible under Article 1(2) of Regulation (EU) 2022/1925, then Article 6(7) of that Regulation applies. Indeed, one of the key objectives of Regulation (EU) 2022/1925 is to foster and promote innovation in the digital sector and remove barriers that could prevent market participants from innovating.⁶² Specifically, Article 6(7) of Regulation (EU) 2022/1925 aims to allow third parties to develop and provide innovative services or hardware complementing or supporting the designated operating system offered by a gatekeeper.⁶³ Such innovation can only take place if interoperability is not limited to a select group of beneficiaries, apps or use cases. In particular, it cannot be left to the discretion of the gatekeeper to decide which third parties, apps, products and use cases can benefit from the interoperability mandated by Article 6(7) of Regulation (EU) 2022/1925, whether through discriminatory restrictions of any nature or the outright exclusion of beneficiaries, apps, or use cases.

⁶¹ In its reply to the Preliminary Findings, footnote 97, Apple claims that according to the Preliminary Findings, Apple shall only provide third-party access to certain future functionalities when these features will become available to Apple in the EU. The Preliminary Findings do not contain such a statement. Such a statement is not supported by the any of the provisions of Regulation (EU) 2022/1925 and its geographic scope, the language of Article 6(7) of that Regulation and it would be inconsistent with the goal of this provision to enable innovation by third parties.

⁶² See, for example, recitals 4, 32 and 107 of Regulation (EU) 2022/1925.

⁶³ Recital 57 of Regulation (EU) 2022/1925.

- (76) According to Apple, Article 6(7) of Regulation (EU) 2022/1925 only requires Apple to provide interoperability to a third party that is a competitor of an Apple service or hardware in the Union. To support its interpretation, Apple refers to recitals 55 and 57 of Regulation (EU) 2022/1925, which mention “*competing service or hardware providers*” and “*competing third parties*” respectively.⁶⁴
- (77) Apple’s restrictive interpretation of Article 6(7) of Regulation (EU) 2022/1925 is not supported by the language or aim of that provision.
- (a) *First*, the language of Article 6(7) of Regulation (EU) 2022/1925 does not contain any limitations on the eligibility of beneficiaries, apps and use cases of this provision. It simply refers to “*providers of services and providers of hardware*.” An interpretation of the recitals cannot limit the scope of the relevant operative provision.⁶⁵
 - (b) *Second*, as described above, Article 6(7) of Regulation (EU) 2022/1925 aims at promoting innovation by opening up access to operating system features which currently operate as a gate and lock end users into gatekeepers’ ecosystems. If interoperability were to be limited to those services and hardware that a gatekeeper already offers, the gatekeeper would enjoy a first-mover advantage for every use case relying on reserved iOS features, leaving little room for innovation. It would be up to the gatekeeper to determine which new services or hardware are in the scope of the obligation. This would effectively cap innovation at the level of the gatekeeper and tie innovation to the moment in time when the gatekeeper decides to use the available iOS features to offer a specific use case – if ever. Third parties must be granted interoperability especially for novel and new innovative products and services that the gatekeeper does not yet offer to be able to “*overcome barriers to entry*” and “*challenge the gatekeeper on the merits of their products and services*.”⁶⁶
 - (c) *Third*, Article 6(7) of Regulation (EU) 2022/1925 applies to features “*as are available to, or used by*” the gatekeeper’s services and hardware, rather than only to features *used by* the gatekeeper’s services and hardware. If this provision would only apply to the same services and hardware as the gatekeeper is offering in competition with a third party, there would be no need to also cover features *available to* but not *used by* the gatekeeper. Instead, the language of Article 6(7) of Regulation (EU) 2022/1925 makes clear that once a feature is available to a service or hardware of the gatekeeper, that feature must be made interoperable for third-party services or hardware.
 - (d) *Fourth*, the reference to “*competing*” in recitals 55 and 57 of Regulation (EU) 2022/1925 does not support Apple’s proposed interpretation. Recital 55 of that Regulation discusses competing providers in a situation in which the gatekeeper already provides services or hardware, such as wearable devices, for which competing providers exist. It does not discuss other situations. Recital 57 of Regulation (EU) 2022/1925 refers, most prominently, to

⁶⁴ Apple’s reply to the Preliminary Findings, Sections I.B. and V.F.a.

⁶⁵ In any case, recitals 55 and 57 of Regulation (EU) 2022/1925 cannot be interpreted as suggesting that “*competing*” implies defining markets. Such an interpretation would be contrary to the objectives of Regulation (EU) 2022/1925. In this regard it is worth recalling that recital 23 of Regulation (EU) 2022/1925 excludes the relevance of market definition in the context of designation. See judgment of 17 July 2024, Bytedance Ltd, T 1077/23, EU:T:2024:478, paragraphs 45-46.

⁶⁶ Recital 32 of Regulation (EU) 2022/1925.

“*alternative*,” not competing service and hardware providers, and of the gatekeeper’s “*complementary or supporting*” services or hardware. These references do not mean that Article 6(7) of Regulation (EU) 2022/1925 limits interoperability to third-party services or hardware that are identical to the ones of the gatekeeper. It rather emphasises the general purpose of Article 6(7) of Regulation (EU) 2022/1925, namely, to be able to rely on a designated operating system’s features to foster and promote innovation in the digital sector and remove barriers that could prevent market participants from innovating.

- (e) *Fifth*, Apple’s contention that Article 6(7) of Regulation (EU) 2022/1925 is limited to competing services or hardware, with the implication, according to Apple, that these provisions should be applied on a case-by-case basis depending on whether a concerned third party is, or is not, competing with Apple’s own services or hardware, would require a definition of the relevant market and an analysis of the actual or potential competition between a given set of product and service offerings. Such a situation would not be consistent with recital 5 and 11 of Regulation (EU) 2022/1925, according to which this Regulation aims to ensure fair and contestable markets, independently from the actual, potential or presumed effects of the conduct of a given gatekeeper on competition in a given market. The legislators’ intention is to avoid pursuing an extensive investigation of complex facts so as to allow for a swift implementation of the Regulation towards its beneficiaries.

3.1.5. *Interoperability must be effective*

- (78) Interoperability under Article 6(7) of Regulation (EU) 2022/1925 needs to be effective, meaning that it must enable the desired result to be achieved in practice. As such, the interoperability solution must be granted in a manner that is technically sound, stable, and workable in practice for third parties without unnecessary hurdles, be they on the side of third-party providers or on the side of end users.
- (79) The gatekeeper must enable third parties to interconnect smoothly through interfaces or similar solutions to the respective features. For this purpose, the gatekeeper may have to technically develop and implement such interfaces (e.g. application programming interfaces (“APIs”)⁶⁷ or other solutions), to ensure that the features subject to Article 6(7) of Regulation (EU) 2022/1925 work with the hardware and software of third parties in all the ways in which they are intended to function. This means that for an interoperability solution to be effective, the solution that a gatekeeper has to make available to third parties may in some cases go beyond merely making an interface available to third parties. As such, this might require, for instance, the use of technical standards, the provision of technical documentation or assistance, or the provision of software development kits (“SDKs”), which are commonly used to achieve interoperability.⁶⁸
- (80) In addition, for interoperability to be effective in practice, gatekeepers cannot be circumventing it through practices that may render an interoperability solution

⁶⁷ See recital (131) of this Decision.

⁶⁸ For instance, Apple makes available the iOS SDK, which app developers must use for software development for iOS devices. See e.g. <https://developer.apple.com/documentation/ios-ipados-release-notes/ios-ipados-18-release-notes>: “The iOS & iPadOS 18 SDK provides support to develop apps for iPhone and iPad running iOS & iPadOS 18,” accessed on 15 November 2024.

ineffective, such as imposing conditions that unduly differentiate between third parties; imposing conditions that are not equal to those that apply to the gatekeeper's own services and hardware; failing to properly consider the needs of third parties that will make use of the solution, e.g. by implementing limitations that prevent certain use cases; providing implementations that are not properly tested for bugs or other shortcomings (e.g. design gaps, performance and stability issues); providing implementations that are less stable or consistent over time than the feature used by or available to the gatekeeper; failing to provide adequate and up-to-date documentation; or failing to provide adequate and timely assistance to third parties that report issues (e.g. by submitting bug reports).

- (81) In this context the Commission also notes that for an interoperability solution to be effective, the solution must take account of how the third party making use of the solution makes its services available to its end users and with the possible involvement of other third parties. As such, the interoperability solution should not impose undue costs – including development costs – for third parties directly benefitting from the interoperability solution or for other third parties that are involved in the use of the relevant feature.⁶⁹ For instance, when notifications received on a smartphone are also displayed on a connected smartwatch, three parties are involved: the operating system (provided by the gatekeeper), the smartwatch provider, as well as providers of apps that post notifications, such as messaging apps. These apps that post notifications use existing operating system APIs that may currently (only) support the gatekeeper's own connected physical devices *out-of-the-box*, i.e. without the need to implement any modification to support them. The developers of these apps would want to continue using the same APIs to interconnect with other smartwatch providers. Indeed, developers of apps posting notifications would have limited incentives to switch to or to add support for different APIs, only to facilitate interoperability for other third parties (such as smartwatch providers), as this would entail additional development costs that such app developers would be unlikely to bear. Therefore, if an interoperability solution for some third parties were to require *other* third parties (e.g. messaging app providers) to adapt their apps to make the solution workable in practice, this would *de facto* shift the burden of compliance from the gatekeeper to those third parties, in breach of the obligation for the gatekeeper to ensure effective interoperability under equal conditions.⁷⁰

⁶⁹ These third parties may not necessarily be business users of the third parties that benefit from the interoperability solution. For example, when a notification from a messaging app is displayed on a smartwatch, this is made possible by the technical implementation of the operating system, which acts as an intermediary. It is not required – and normally it is not the case – that the messaging app developer and the smartwatch provider are in a professional relationship, or even that they are aware of each other's products.

⁷⁰ For example, on iOS, many messaging apps currently use a specific set of iOS APIs to post notifications. These APIs are interoperable out-of-the-box for the Apple Watch: messaging apps providers do not need to write any custom code to ensure that the notification is displayed on the Apple Watch. Such out-of-the-box support should be available to third-party smartwatch providers too. Indeed, if every messaging app provider – including Apple itself, which provides apps posting notifications, such as the Mail app – was required to develop custom support to display notifications on third-party smartwatches, this would be outside of the control of any third-party smartwatch provider (the beneficiary). This requirement would therefore shift the burden of compliance onto messaging app providers and create a “chicken and egg” situation: on one hand, messaging app providers (which are not the relevant beneficiaries of the interoperability solution) may have low incentives to devote efforts to develop custom code for third-party smartwatches, given that they currently have low adoption

- (82) Especially on the side of end users, the effectiveness of interoperability solutions could be undermined by introducing unnecessary “friction” when an end user uses third-party services or hardware. Friction refers to any obstacle, difficulty, or inefficiency that hinders or affect the end user’s ability to complete a task or achieve their goal in the shortest possible time and with the least effort. Friction has an impact on the ease, convenience and speed of using the connected physical device and related apps from the end user perspective. Friction is unnecessary if it is imposed by the operating system only on end users of third-party services and hardware, but not on end users of the gatekeeper’s services and hardware.
- (83) While Apple argues that Article 6(7) of Regulation (EU) 2022/1925 does not support any requirement regarding friction, such a requirement follows directly from “effectiveness” and “equal conditions”. Indeed, it is well known that adding only a small amount of friction can have an outsized impact on end user behaviour and ultimately on commercial success.⁷¹ Digital service providers often employ teams and tools to study user behaviour and minimise or, in some cases, maximise friction.⁷²
- (84) A user experience without unnecessary friction is essential to enable a level playing field between third-party and gatekeeper’s connected physical devices. End users expect a frictionless experience. Friction makes it more likely that an end user will abandon a user journey that is necessary to use some functionalities of their connected physical device or related services, e.g. setting up, using, or configuring the device.⁷³ Unnecessary friction undermines effective interoperability, as end users may not enjoy the full functionality of a third-party connected physical device, in turn reducing the commercial attractiveness of those devices. The avoidance of friction and the seamlessness of a user journey is critical to improving the user experience, i.e. “the overall experience users have [...], which includes the perceived utility, ease of use and efficiency of interacting with it [e.g. the connected physical device].”⁷⁴
- (85) Friction is introduced by measures that make the “user journey” – i.e. “the series of actions or steps for users to perform in order to reach their goal”⁷⁵ – slower or more complicated and frustrating than necessary. Friction can be caused by any

among iOS users; on the other hand, third-party smartwatches would remain less attractive to end users until they are supported by at least the most popular messaging apps.

⁷¹ For example, Google explains that when a website “reduce[d] load times from nine seconds to 1.4 seconds, ad revenue increased three percent, and page views-per-session went up 17 percent” and that “[w]hen you speed up service, people become more engaged - and when people become more engaged, they click and buy more,” see <https://www.thinkwithgoogle.com/future-of-marketing/digital-transformation/the-google-gospel-of-speed-urs-hoelzle/>, accessed on 24 February 2025.

⁷² <https://www.thealien.design/insights/ux-metric>, accessed on 24 February 2025.

⁷³ [Third-party developer]’s submission of 4 October 2024, paragraph 1.

⁷⁴ See “Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them,” European Data Protection Board, version 2.0, 2023, https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf, accessed on 15 November 2024.

⁷⁵ See “Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them,” European Data Protection Board, version 2.0, 2023, https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf, accessed on 15 November 2024.

behavioural techniques or interface design elements that force an end user to take several, potentially confusing actions before the end user can use a service or complete a task. Examples of such techniques are successive and excessive permission prompts, or unnecessary requirements to switch app to complete an operation.

- (86) Friction can also be caused by offering choices to the end user in a non-neutral manner that steers the end user towards making certain choices, or by limiting the ability to exercise its choice effectively and easily. Examples of such techniques are misrepresenting the risks of using the connected physical device or communicating risks based on the mere theoretical possibility that such risks might materialise. Another example is the practice of disabling by default a permission that is necessary for the proper and full functioning of the connected physical device and requiring the user to actively search for the option in settings in order to change it.
- (87) Regulation (EU) 2022/1925 recognizes the harmful impact of friction and its detrimental effect on contestability and fairness. Recital 37 of Regulation (EU) 2022/1925 provides that “*gatekeepers should not design, organise or operate their online interfaces in a way that deceives, manipulates or otherwise materially distorts or impairs the ability of end users to freely give consent.*” Further, it requires that “*not giving consent should not be more difficult than giving consent*” and that the gatekeeper “*should proactively present a user-friendly solution to the end user to provide, modify or withdraw consent in an explicit, clear and straightforward manner.*” Articles 13(4) and (6) of Regulation (EU) 2022/1925 recognise that friction undermines effective compliance, including via the use of behavioural techniques or interface design and by making the exercise of those rights or choices unduly difficult, including by offering choices to the end user in a non-neutral manner, or by subverting end users’ or business users’ autonomy, decision-making, or free choice via the structure, design, function or manner of operation of a user interface or a part thereof.
- (88) Equally effective interoperability requires that end users can set preferences (i.e. settings) in relation to third-party services and hardware as they can for the gatekeeper’s services and hardware. To allow the end user to configure a specific setting, there are generally two options for the location of these settings: to include the setting in system-level settings,⁷⁶ or to have it inside the app provided by the third party (or both). For example, the settings to enable do-not-disturb mode at night on a connected physical device may be located in system-level settings or in the companion app of the device.⁷⁷ If the end user is required to switch between a third-party app and the system-level settings in order to change relevant settings, this may add significant friction compared to the use of the gatekeeper’s services or hardware, in particular if not clearly directed to the relevant setting.⁷⁸ Therefore, when the gatekeeper designs the interoperability solution, it should ensure that the location and design of the relevant settings: (i) do not make the user experience more burdensome

⁷⁶ See definition in recital (140) of this Decision.

⁷⁷ A companion app is an iOS app that facilitates the use of connected physical devices – see definition in recital (137) of this Decision.

⁷⁸ It is often difficult for the end user to locate and change the setting in system-level settings, if the relevant setting is not highlighted and the end user is not guided back to the third-party app.

for end users of third-party services and hardware; and (ii) are sufficiently flexible to meet reasonable differentiation needs of different third parties.⁷⁹

- (89) Contrary to what Apple claims, the measures in this Decision neither require Apple to remove friction from, nor to ensure the functioning or the attractiveness of the services or hardware of third parties.⁸⁰ Apple is only required to ensure effective interoperability under equal conditions. In the context of friction, this means that Apple is only required not to add, directly or indirectly, friction with regard to third parties that does not exist for its own services and hardware.
- (90) Apple submits that Article 6(7) of Regulation (EU) 2022/1925 speaks of “*allowing*” interoperability, which is limited to permit the interconnection with features, but does not entail a duty to create new technologies or additional engineering work.⁸¹
- (91) This Decision requires Apple to ensure that third-party services and hardware can access or interoperate with some existing features controlled by or accessed via iOS, and not to create new features. However, the Decision may require additional engineering work to make the those features interoperable.
- (92) The above interpretation is fully in line with the language and aim of Article 6(7) of Regulation (EU) 2022/1925, which are focused on one result, namely effective interoperability with the same feature under equal conditions, but not necessarily with the same software implementation (see Section 3.1.1 of this Decision). *First*, interoperability itself is a results-based concept, where, as per the definition of “interoperability” in Article 2(29) of Regulation (EU) 2022/1925, “*all elements of hardware or software work with other hardware and software and with users in all the ways in which they are intended to function.*” Regulation (EU) 2022/1925 therefore makes it clear that a gatekeeper may have to undertake certain engineering work to make an interoperability solution available to third parties. The definition also provides that information shall be exchanged “*through interfaces or other solutions.*” Recital 57 of Regulation (EU) 2022/1925 explains that the gatekeeper should “*allow competing third parties to interconnect through interfaces or similar solutions to the respective features.*” Recital 57 of Regulation (EU) 2022/1925 further clarifies that a gatekeeper is “*required to ensure [...] effective interoperability.*” *Second*, the verb “*allow*” does not intrinsically refer only to a passive action. Instead, “*allow*” defines an endpoint of “*making it possible for something to be done or to happen,*”⁸² in this case interoperability with the same features as available to the gatekeeper.⁸³
- (93) What an effective interoperability solution requires depends on the gatekeeper’s choices regarding the design of its operating system. For some features a mere lifting

⁷⁹ For example, for the do-not-disturb mode, a flexible solution may be to surface the system-level do-not-disturb mode setting to the third-party companion app, so that the third party may decide whether to automatically apply it to the connected physical device, or whether to have a separate setting that allows the end user to have more granular control over do-not-disturb mode for that specific connected physical device. For some features, this Decision specifies the location of relevant settings.

⁸⁰ Apple’s reply to the Preliminary Findings, paragraph 96, see also paragraphs 69, 65, 38.

⁸¹ Apple’s reply to the Preliminary Findings, paragraphs 59-61.

⁸² See Cambridge Dictionary, <https://dictionary.cambridge.org/dictionary/english/allow>, accessed on 24 February 2025.

⁸³ The above interpretation is also in line with the judgment *Alphabet v AGCM*, where the Court of Justice held that granting interoperability can entail the adoption of additional work, such as the development of a template to implement a requested interoperability for certain third-party apps. See judgment of 25 February 2025, *Alphabet v AGCM*, C-233/23, ECLI:EU:C:2025:110, paragraphs 73-74.

of a contractual or technical restriction might be sufficient. In other cases, the gatekeeper might need to implement the prerequisites – including software components – that are required to provide effective interoperability.

- (94) Apple’s argument is also inconsistent insofar as Apple itself asks to be able to build new and separate interoperability solutions for third parties because some of the solutions available to Apple would not be suitable for third parties.⁸⁴ [...]

3.2. Innovation

- (95) A main goal of Article 6(7) of Regulation (EU) 2022/1925 is to enable innovation by third parties. Recital 57 of that Regulation explains that a lack of interoperability under equal conditions could significantly undermine innovation by alternative providers. A level playing field allows fair competition, which in turn creates incentives for innovation.⁸⁵ Apple claims that the Commission’s measures will suppress innovation. Apple argues that requiring to make its proprietary technologies available to developers for free deprives Apple of its ability to build and monetise differentiating products.⁸⁶ Contrary to Apple’s claims, the measures in this Decision will enable innovation by alternative providers and will create more incentives also for Apple to innovate.
- (96) Article 6(7) of Regulation (EU) 2022/1925 is designed to ensure that complementary and supporting services by the gatekeeper cannot enjoy exclusive or privileged access to operating system features compared to third-party complementary and supporting services. Access to features under equal conditions fosters contestability and fairness for business users dependent on the gatekeeper’s operating system as a gateway by lowering barriers to entry and expansion.⁸⁷ Such contestability and fairness, in turn, improve the innovation potential of the wider online platform economy, *inter alia* by preventing unfair practices by gatekeepers in relation to their CPS.⁸⁸
- (97) The measures in this Decision enable such innovation. For example, access to iOS notifications will put third-party smartwatches on a more level playing field with the Apple Watch, enabling them to compete with the Apple Watch on other aspects – such as design and battery life – and incentivising Apple to innovate on the same or other aspects.
- (98) The measures specified by the Commission will also indirectly increase Apple’s incentives to innovate within iOS itself. More contestability for complementary or supporting services or hardware will bring more contestability for operating systems. The measures will improve interoperability of third-party connected physical devices, for example smartwatches, with iOS, thus allowing such products to compete more fairly with Apple’s services and hardware, for example the Apple Watch, potentially attracting more buyers. Unlike the owners of Apple’s connected physical devices, these owners of third-party services and hardware are not locked

⁸⁴ Apple’s reply to the Preliminary Findings, Section II.B.

⁸⁵ See Competition and Markets Authority, *Mobile ecosystems market study: Final report*, Section 7, <https://www.gov.uk/government/publications/mobile-ecosystems-market-study-final-report>, accessed on 24 February 2025.

⁸⁶ Apple’s reply to the Preliminary Findings, Section II.C and paragraph 101.

⁸⁷ Recitals 32, 33, 34 and 57 of Regulation (EU) 2022/1925.

⁸⁸ Recital 32 of Regulation (EU) 2022/1925.

into Apple's ecosystem⁸⁹ and are able to switch more easily to third-party smartphones. Thus, an increased number of owners of third-party connected physical devices will increase Apple's incentives to bring innovation within iOS to attract consumers to buy and continue using iPhones.

- (99) Finally, the existence of more open ecosystems shows that interoperability does not preclude innovation nor its monetisation. Apple can continue to build and monetise differentiating products using the features subject to this Decision. These products will be differentiated *inter alia* by Apple's proprietary branding and design. Providers of operating systems that are mostly interoperable by design have been able to continue to innovate, and so have the providers of complementary and supporting services for these operating systems.⁹⁰

3.3. Integrity justification

- (100) According to Article 6(7) of Regulation (EU) 2022/1925, the gatekeeper shall not be prevented from taking strictly necessary and proportionate measures to ensure that interoperability does not compromise the integrity of the operating system, virtual assistant, hardware or software features provided by the gatekeeper, provided that such measures are duly justified by the gatekeeper.
- (101) Recital 50 of Regulation (EU) 2022/1925 clarifies that the integrity of the hardware or the operating system includes 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.
- (102) Within the architecture of Regulation (EU) 2022/1925, integrity has a distinct meaning from users' privacy and security. While a measure to ensure that interoperability does not compromise the integrity of the operating system, virtual assistant, hardware or software features provided by the gatekeeper ("integrity measure") may have positive effects on the privacy or security of the user, the legislator clearly distinguished these concepts in the context of Regulation (EU) 2022/1925, making them appear in different provisions, namely Articles 7(9) and 6(4) of that Regulation.⁹¹ As regards security, recital 50 of Regulation (EU) 2022/1925 describes security and integrity differently, referring to "*end users' security*", indicating that security can be seen as pertinent to the end user. Similarly, recital 72 of Regulation (EU) 2022/1925 describes privacy (and data protection) as "*interests of end users*".

⁸⁹ For example, when an iPhone user owns an Apple Watch and wants to buy a new smartphone, the switching costs to switch to a non-Apple smartphone are higher than just buying a new iPhone. Indeed, because the Apple Watch does not work with non-Apple smartphones, the user would need to buy also a new smartwatch that works with the non-Apple smartphone. This phenomenon is what Apple itself calls the "*stickiness*" of Apple's ecosystem – see *United States v. Apple Inc., No. 1:24-cv-00783* (D.D.C. 2024), pages 6, 30, 68, <https://www.justice.gov/archives/opa/media/1344546/dl?inline>, accessed on 24 February 2025.

⁹⁰ See Competition and Markets Authority, *Mobile ecosystems market study: Final report*, Section 7, <https://www.gov.uk/government/publications/mobile-ecosystems-market-study-final-report>, accessed on 24 February 2025.

⁹¹ In a lawsuit against Apple, the US Department of Justice has already identified the risk of overly flexible concepts of privacy and security, claiming that "*Apple deploys privacy and security justifications as an elastic shield that can stretch or contract to serve Apple's financial and business interests.*" See *United States v. Apple Inc., No. 1:24-cv-00783* (D.D.C. 2024), p. 12, <https://www.justice.gov/archives/opa/media/1344546/dl?inline>, accessed on 24 February 2025.

- (103) By contrast, Regulation (EU) 2022/1925 does not apply integrity as an attribute or property of end users, but only as a property of services and of their features.⁹² A pertinent definition of integrity is the state of being unimpaired of such service or feature – that is, still functional and not damaged nor corrupted. Regulation (EU) 2024/2847 (Cyber Resilience Act)⁹³ links integrity to the absence of manipulation or modification not authorised by the user.⁹⁴ The records of the legislative process that led to the adoption of the Regulation (EU) 2022/1925 indicate that the legislator has considered but ultimately rejected the position that cyber security and end user data protection may serve as a justification. Instead, it decided in favour of a justification grounded on integrity only.⁹⁵
- (104) Therefore, in the context of Article 6(7) of Regulation (EU) 2022/1925, the concept of integrity encompasses the risks which threaten to impair the correct functioning of the gatekeeper’s operating system, or hardware or software features provided by the gatekeeper, including of security controls designed to prevent unauthorised access to the operating system or these features which might compromise their integrity.⁹⁶ User authorisation may in certain cases be sufficient to address an integrity concern.⁹⁷ This is consistent with the goal of Article 6(7) of Regulation (EU) 2022/1925 to enable user choice and innovation by alternative providers of services,⁹⁸ and is consistent with the functioning of operating systems as a platform for third-party apps and services. Indeed, Article 6(7) of Regulation (EU) 2022/1925 aims at providing access to features that are important for third-party innovation and therefore only allows gatekeepers to take measures that are strictly necessary and duly justified to ensure interoperability does not compromise integrity of the operating system, hardware and the features at stake. Such third-party innovation may include novel types of services and hardware that the gatekeeper does not (yet) provide, but which rely on access to features accessed or controlled via operating system.

⁹² Similarly, in *Alphabet v AGCM*, within the context of Article 102 TFEU, the Court of Justice made clear that a dominant undertaking may not need to provide an interoperability solution if it compromises the integrity or security of “the platform concerned” but does not refer to the integrity or security of the end user (see judgment 25 February 2025, C-233/23, ECLI:EU:C:2025:110, paragraph 73).

⁹³ Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).

⁹⁴ Annex I Part I paragraph 2 of Regulation (EU) 2024/2847 provides that “products with digital elements shall: [...] (f) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions.”

⁹⁵ During the legislative process, the European Parliament’s position before the Trilogue included a justification allowing for integrity, end user data protection and cyber security grounds, see P9_TA(2021)0499, Amendments adopted by the European Parliament on 15 December 2021 on the proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) (COM(2020)0842 – C9- 0419/2020 – 2020/0374(COD)). The Union legislator rejected this position in favour of an integrity justification.

⁹⁶ See, by analogy, judgment of 17 September 2007, *Microsoft v Commission*, T-201/04, EU:T:2007:289, paragraphs 1165 and 1220.

⁹⁷ Annex I Part I paragraph 2 of Regulation (EU) 2024/2847 provides that “products with digital elements shall: [...] (f) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions.”

⁹⁸ Recital 57 of Regulation (EU) 2022/1925.

- (105) In this respect, the Commission notes that compliance with specific obligations in the areas of data protection and security falls within the competence of the public authorities in charge of those respective sectors. Both Apple and the providers of services or hardware requesting effective interoperability under Article 6(7) of Regulation (EU) 2022/1925 are subject to legal obligations applicable to their activities concerning, *inter alia*, security or privacy. The Commission further notes that Article 6(7) of Regulation (EU) 2022/1925 shall be interpreted in conformity with the principle of proportionality and the fundamental rights guaranteed in the Charter of Fundamental Rights of the European Union.
- (106) The Commission considers that, in some circumstances, protecting integrity can bring benefits for end users' security and privacy. Indeed, integrity measures are used to ensure that security and privacy controls are not manipulated without the end user's authorisation. For example, integrity measures can ensure that no app can unduly disable an end user's passcode to unlock the screen, preventing unauthorised access and increasing security. Similarly, when a map app triggers a system prompt to obtain the end user's permission for access to GPS location, integrity measures may prevent a malicious actor from manipulating the prompt, to ensure that it is the end user who makes the actual choice about the end user's privacy.⁹⁹ The same applies to every security and privacy control ensuring that choices made by end users are respected, such as: access to camera, microphone, or photos depending on the app; enforcing automatic VPN connections on certain Wi-Fi networks; or use of biometrics to unlock the phone. Integrity ensures that these controls function without manipulation or corruption, including by malware.
- (107) However, some privacy and security aspects fall outside the scope of integrity within the meaning of Regulation (EU) 2022/1925. In particular, the concept of integrity in Regulation (EU) 2022/1925 does not allow gatekeepers to impose their own model of security and privacy on third-party services. Indeed, nothing in Regulation (EU) 2022/1925 precludes competition or differentiation in relation to models of security and privacy, as long as they are compliant with applicable legislation. For example, the gatekeeper should not prevent third-party apps from accessing the smartphone's camera if they have obtained user's consent – as access to the camera is necessary for many legitimate use cases, such as video conferencing apps. Therefore, given that third-party services and hardware remain subject to applicable legislation, including on data protection and cyber security, the choice whether to use a service should be the prerogative of the end user, not of the gatekeeper controlling the operating system.
- (108) Under Regulation (EU) 2022/1925, the burden is on the gatekeeper to duly justify how the measures it intends to take to mitigate any integrity risk are necessary and proportionate in the context of the implementation of the effective interoperability. It is the gatekeeper, having the full knowledge of its own operating system, who is best placed to detect any risks to the integrity of its operating system resulting from interoperability access and to propose and duly justify specific measures to ensure that integrity is not compromised. In practice, to discharge this burden, gatekeepers

⁹⁹ In this example, the permission prompt itself is therefore a privacy measure, not an integrity measure. On the other hand, a measure preventing manipulation of the system prompt would be an integrity measure ensuring that the integrity of the operating system and of the feature is not compromised. Modern operating systems employ many such measures, such as hardware-backed integrity, to ensure that system files – including those enforcing privacy prompts – are not manipulated.

ought to substantiate the specific integrity concerns in the context of the operating system in question, the measures it intends to implement to mitigate those risks, how the measures will address the identified integrity risk, why the measures are strictly necessary; and why the measures are proportionate, including considering the extent to which the proposed measure may reduce effective interoperability.

- (109) In doing so, the gatekeeper must demonstrate, in a verifiable way using data or other objective means, the existence and magnitude of the integrity risk.¹⁰⁰ In that respect, evidence regarding how other operating systems deal with the same or similar integrity risk can be relevant.
- (110) To satisfy the standard of strict necessity and proportionality, the gatekeeper must, where there are several available integrity measures that are suitable to achieve the objective of mitigating the integrity risks, select the measure which is least restrictive as regards achieving effective interoperability under Article 6(7) of Regulation (EU) 2022/1925. Proportionality ought to be examined by taking into consideration, in particular, the objectives of Article 6(7) of Regulation (EU) 2022/1925 and that Regulation itself, which necessitates that those objectives be weighed against the objective pursued by the integrity justification in the second subparagraph of that provision. An integrity measure may therefore not be appropriate if it disproportionately limits the attainment of the objective of Article 6(7) of Regulation (EU) 2022/1925 taking into account, for instance, the nature of the integrity concern and availability of alternative measures to mitigate these concerns.¹⁰¹ For instance, asking users, via a permission prompt whether they would like to grant computing power to a specific app may be less restrictive than imposing strict limits on the use of such power resources for all third-party apps for integrity reasons, and only a permission prompt may be appropriate in light of the objective of Article 6(7) of Regulation (EU) 2022/1925 and of that Regulation as a whole.¹⁰²
- (111) Moreover, the Commission considers that an integrity measure 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. Integrity measures can only be proportionate if they are based on transparent, objective, precise and non-discriminatory conditions that apply equally to the gatekeeper's and third parties' services and hardware.¹⁰³ These conditions

¹⁰⁰ By analogy, judgments of 21 December 2023, International Skating Union, C-124/21 P, EU:C:2023:1012, paragraphs 137 and 138 (“verifiable objectives”); of 26 September 2013, Ottica New Line di Accardi Vincenzo, C-539/11, EU:C:2013:591, paragraph 56. See also, by analogy, judgments of 20 March 2014, Commission v. Poland, C-639/11, EU:C:2014:173, paragraph 62; of 20 March 2014, Commission v. Lithuania, C-61/12, EU:C:2014:172, paragraph 67. The case law cited in this section referring to the legal principle of proportionality (including in case law on the EU fundamental freedoms) is relevant since Article 6(7), second subparagraph of Regulation (EU) 2022/1925 imposes a proportionality requirement and typically also refers to the invocation of a justification or exception.

¹⁰¹ By analogy, judgment of 23 December 2015, Scotch Whisky Ass'n, EU:C:2015:845, paragraph 28.

¹⁰² See, by analogy, judgment of 20 February 1979, Rewe-Zentral AG v Bundesmonopolverwaltung für Branntwein (Cassis de Dijon), C-120/78, ECLI:EU:C:1979:42, paragraph 13, where informing customers by way of labelling was considered less restrictive than minimum alcohol content requirements set out by German law.

¹⁰³ By analogy, judgments of 21 December 2023, Superleague, C-333/21, EU:C:2023:1011, paragraphs 135, 147, 254; of 28 February 2013, Ordem dos Técnicos Oficiais de Contas, C-1/12, EU:C:2013:127, paragraphs 84-86, 90, 91, 99.

must be clearly defined.¹⁰⁴ These requirements ensure that the integrity justification is not used arbitrarily.¹⁰⁵ They also ensure that conditions do not discriminate against innovative use cases and innovative types of services and hardware by third parties, including those that the gatekeeper is not yet providing.

- (112) Similarly, to prevent arbitrary limitations on the obligation to allow for effective interoperability under Article 6(7) of Regulation (EU) 2022/1925, the gatekeeper shall only apply conditions whose satisfaction is capable of being independently verified and are not exclusively within the gatekeeper's control. Absent verifiability, the gatekeeper retains broad discretion to abuse its power.¹⁰⁶ Otherwise, the affected third parties, other independent third parties, the Commission, and courts would be incapable of assessing compliance,¹⁰⁷ and the gatekeeper could set conditions which are unachievable by third parties. Such conditions would be intrinsically liable to affect third parties more than the gatekeeper's own services and hardware, with a consequent risk that the gatekeeper would place third parties at a particular disadvantage.¹⁰⁸ Leaving the decision to deny or limit interoperability via the integrity justification entirely to the gatekeeper is liable to affect its objectivity and impartiality.¹⁰⁹
- (113) The Commission also considers that a gatekeeper may not justify an integrity measure implemented in relation to third parties' services or hardware solely based on whether the gatekeeper controls or trusts such third parties. In particular, a gatekeeper may not justify integrity measures by the mere fact that third parties are not the gatekeeper, and therefore they cannot be trusted. This is because whether a gatekeeper trusts a third party is a subjective assessment exclusively within the gatekeeper's control. The requirement of "*gatekeeper's trust*" is a condition that is neither capable of being independently verified, nor objective or precise. A gatekeeper should set out the objective conditions which, in its view, mitigate or remove its integrity concerns and which should be met by its own and third-party

¹⁰⁴ By analogy, judgments of 28 February 2023, *Ordem dos Técnicos Oficiais de Contas*, C-1/12, EU:C:2013:127, paragraph 99; of 16 December 2020, *International Skating Union*, T-93/18, EU:T:2020:610, paragraph 88.

¹⁰⁵ By analogy, judgments of 21 December 2023, *Superleague*, C-333/21, EU:C:2023:1011, paragraph 255; of 22 January 2002, *Canal Satélite Digital*, C-390/99, EU:C:2002:34, paragraph 35; of 13 June 2019, *TopFit and Biffi*, C-22/18, EU:C:2019:497, paragraph 65.

¹⁰⁶ By analogy, judgments of 21 December 2023, *International Skating Union*, C-124/21 P, EU:C:2023:1012, paragraphs 137, 138; of 16 December 2020, *International Skating Union*, T-93/18, EU:T:2020:610, paragraphs 88 ("*authorization criteria must be clearly defined, transparent, non-discriminatory, reviewable and capable of ensuring the organisers of events effective access to the relevant market*"), 118 ("*Given the absence of objective, transparent, non-discriminatory and verifiable authorisation criteria, the applicant's broad discretion to authorise or reject such events was in no way limited.*"), and 129; judgment of 28 February 2023, *Ordem dos Técnicos Oficiais de Contas*, C-1/12, EU:C:2013:127, paragraph 99.

¹⁰⁷ Apple lists as one core requirement for its new service Private Cloud Compute the "*verifiable transparency*" stating that "*researchers need to be able to verify, with a high degree of confidence, that our privacy and security guarantees for Private Cloud Compute match our public promises,*" see <https://security.apple.com/blog/private-cloud-compute/>, accessed on 24 February 2025.

¹⁰⁸ See, by analogy, judgments of 13 April 2010, *Bressol and Others*, C-73/08, EU:C:2010:181, paragraph 41; of 30 November 2000, *Österreichischer Gewerkschaftsbund*, C-195/98, EU:C:2000:655, paragraph 40; of 18 July 2007, *Hartmann*, C-212/05, EU:C:2007:437, paragraph 30.

¹⁰⁹ By analogy, judgment of 10 March 2009, *Hartlauer*, C-169/07, EU:C:2008:478, paragraph 69.

services and hardware – for example, the requirement that apps are appropriately signed by the third party¹¹⁰ and include a “manifest”.¹¹¹

- (114) Moreover, the trust gatekeepers place into their own services and hardware may be misplaced, because a gatekeeper’s own services or hardware may also pose risks for the end user. Indeed, the mere possibility to exercise control does not mean that services or hardware are fully protected against any risk, such as unauthorised access or design or implementation flaws¹¹² invalidating the expected protections.¹¹³ Indeed, vulnerability of apps, services, and operating systems is well documented and providers regularly provide updates to address these vulnerabilities, indicating that despite their efforts, vulnerabilities existed.¹¹⁴ Operating system providers also run programmes enabling and rewarding third parties to identify such vulnerabilities.¹¹⁵ Moreover, insider attacks coming from inside the operating system provider are explicitly considered as a risk to protect against by some operating system providers.¹¹⁶ Finally, the fact that an end user has made the decision to buy a device running the gatekeeper’s operating system does not mean that the end user can be assumed to automatically trust all of the gatekeeper’s services and hardware that interoperate with that operating system. In fact, Article 5(2) of Regulation (EU) 2022/1925 enshrines the principle that end user trust does not automatically extend to all different services provided by the same entity.¹¹⁷

¹¹⁰ See <https://support.apple.com/en-gb/guide/security/sec7c917bfl4/web>, accessed on 24 February 2025.

¹¹¹ An app manifest is a document declaring to the operating system some important information about the app, such as which sensitive features are accessed by the app and the ways in which the app can interact with other apps. See <https://developer.android.com/guide/topics/manifest/manifest-intro>, accessed on 24 February 2025.

¹¹² For example, Apple has recently agreed to pay \$95 million to settle a proposed class action according to which users’ “confidential or private communications were obtained by Apple and/or were shared with third parties as a result of an unintended Siri activation.” See *Lopez v. Apple, Inc.*, 4:19-cv-04577-JSW (N.D. Cal.), Document 336-2, <https://cdn.arstechnica.net/wp-content/uploads/2025/01/Lopez-v-Apple-Proposed-Settlement-Agreement-12-31-2024.pdf>, accessed on 24 February 2025.

¹¹³ See, by analogy, judgment of 24 January 2023, *Stanleybet*, C-186(11) a.o., EU:C:2013:33, paragraphs 33-36, requiring that, for national legislation reducing opportunities for gambling to be lawful under Union law, it must be ensured that public authorities exercise effective and strict controls.

¹¹⁴ For instance, Apple has self-reported 11 991 vulnerabilities of its products to the National Vulnerabilities Database maintained by the US National Institute of Standards and Technology: https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&isCpeNameSearch=false&cpe_vendor=cpe%3A%2F%3Aapple, accessed on 24 February 2025.

¹¹⁵ For instance, under the Apple Security Bounty Apple promises a monetary reward of up to US\$ 2 million for identifying vulnerabilities (see <https://security.apple.com/bounty/>, accessed on 24 February 2025). Microsoft (<https://www.microsoft.com/en-us/msrc/bounty>, accessed on 24 February 2025) and Google (<https://bughunters.google.com>, accessed on 24 February 2025) have similar programmes.

¹¹⁶ For example, Google employees write: “[Insider] attacks can occur at many more levels in the complex supply chain of hard- and software vendors, including [...] malicious insiders at the platform vendor (i.e. Google). [...] Another class of supply chain attacks are organizational attacks on a legal or political level. These may for example take the form of compelled technical insider attacks [...]. The possibility of insider and/or organizational attacks at many levels is an effect of the ecosystem size, and such attacks need to be part of a realistic threat model.” See *The Android Platform Security Model* (2023), <https://arxiv.org/pdf/1904.05572v3>, accessed on 24 February 2025.

¹¹⁷ Article 5(2) of Regulation (EU) 2022/1925 and principles of data protection in EU law and established data protection practices reject the idea that end user trust automatically extends to different services provided by the same entity. For example, the legal basis (including consent) for a certain processing operation does not automatically extend to any processing operation carried out by the same controller – even more so if the processing operations are carried out for different purposes by distinct services,

- (115) A condition or integrity measure is only suitable to achieve the objective of mitigating integrity risks if it genuinely reflects a concern to attain integrity in a consistent and systematic manner.¹¹⁸ This requirement ensures that the condition or measure is suitable to attain the objective of protecting integrity rather than using the integrity justification as a means of arbitrary discrimination or a disguised restriction. Instances where this requirement may not be met include where the gatekeeper allows the particular integrity risk to persist in other areas, undermining the attainment of the goal¹¹⁹ – either technically or due to lack of enforcement or monitoring¹²⁰ – or where the measure is not effective in reaching the goal,¹²¹ which requires assessing the effects of the measures even after their adoption.¹²²

3.4. Legal boundaries of Article 6(7) and 8(2) of Regulation (EU) 2022/1925

- (116) Apple argued that an implementing act under Article 8(2) of Regulation (EU) 2022/1925 may merely specify the content of Article 6(7) of that Regulation by determining the detailed rules for its application, but must not lay down substantive obligations (or alternations thereof), alter the normative content of Article 6(7) of that Regulation or its scope of application.¹²³ Further, Apple submitted that an implementing act under Article 8(2) of Regulation (EU) 2022/1925 must be necessary to ensure “*uniform conditions*” for the implementation of Article 6(7) of that Regulation.¹²⁴
- (117) Article 8(2) of Regulation (EU) 2022/1925 empowers the Commission to specify the measures that the gatekeeper concerned is to implement in order to effectively comply with the obligations laid down in Articles 6 and 7 of that Regulation.¹²⁵ The measures shall be effective in achieving the objectives of Regulation (EU) 2022/1925 and of the relevant obligation.¹²⁶ The Commission may therefore specify any measures that fall within the scope of Article 6(7) of Regulation (EU) 2022/1925 and ensure effective compliance with the objectives of these provisions and of that Regulation as a whole.
- (118) The normative content of Article 6(7) of Regulation (EU) 2022/1925 is not affected by a specification decision. Nor does Article 8(2) of Regulation (EU) 2022/1925 contain a distinction between substantive and non-substantive measures, which would be incompatible with the goal of specification proceedings to ensure that

even if provided by the same controller. Article 5(2) of Regulation (EU) 2022/1925 enshrines the same legal principle by requiring specific consent for data combination and cross-use.

¹¹⁸ Judgments 21 December 2023, *Superleague*, C-333/21, EU:C:2023:1011, paragraph 251; of 8 September 2009, *Liga Portuguesa de Futebol Profissional and Bwin International*, C 42/07, EU:C:2009:519, paragraph 61; of 6 October 2020, *Commission v Hungary (Higher education)*, C 66/18, EU:C:2020:792, paragraph 178; of 10 March 2009, *Hartlauer*, C-169/07, ECLI:EU:C:2009:141, paragraph 55.

¹¹⁹ Judgments of 17 July 2008, *Corporación Dermoestética*, C-500/06, EU:C:2008:421, paragraphs 39-40; of 10 March 2009, *Hartlauer*, C-169/07, EU:C:2008:478, paragraphs 60-63; of 23 December 2025, *Hiebler*, C-293/14, EU:C:2015:843, paragraphs 65-78.

¹²⁰ See judgments of 24 January 2023, *Stanleybet*, C-186(11) a.o., EU:C:2013:33, paragraphs 33-36.

¹²¹ Judgments of 11 June 2015, *Berlington a.o.*, C-98/14, EU:C:2015:386, paragraphs 71 and 72 in particular; of Jose Manuel Blanco Perez, C-570/07 & C-571/07, EU:C:2010:300, paragraphs 101-102.

¹²² Judgments of 30 June 2016, *Admiral Casinos*, Case C-464/15, EU:C:2016:500, paragraphs 34, 36-37; of 23 December 2015, *Scotch Whisky Ass'n*, EU:C:2015:845, paragraphs 60 to 65.

¹²³ Apple's reply to the Preliminary Findings, paragraphs 32-36.

¹²⁴ Apple's reply to the Preliminary Findings, footnote 14.

¹²⁵ See also recital 65 of Regulation (EU) 2022/1925.

¹²⁶ See Articles 8(7), (1), (3) of Regulation (EU) 2022/1925.

gatekeepers effectively comply with that Regulation. Moreover, Apple fails to provide any authority in the relevant case law for its proposition that, when the Commission is called upon to provide further details in relation to the content of a legislative act, as it does when adopting a specification decision under Article 8(2) of Regulation (EU) 2022/1925, these details should pertain only to “*non-substantive*” matters. Finally, by specifying the measures to be taken by Apple to ensure effective compliance with Article 6(7) of Regulation (EU) 2022/1925, the Commission ensures these provisions will be implemented under uniform conditions throughout the European Union.

- (119) Effective enforcement of Regulation (EU) 2022/1925 ensures that it can be implemented under uniform conditions in all Member States.¹²⁷ The measures in this Decision are necessary and appropriate for the implementation of Regulation (EU) 2022/1925 and consistent with the goal of Article 6(7) of that Regulation and of that Regulation as a whole.¹²⁸

4. REQUESTS FOR INTEROPERABILITY CONCERNING CONNECTED PHYSICAL DEVICES

- (120) As explained in recital (5) of this Decision, Apple received several requests for effective interoperability under Article 6(7) of Regulation (EU) 2022/1925 that concern connected physical devices.
- (121) Specifically, the Commission considers the following requests to be of particular relevance for the features concerned by this Decision.
- (a) In January 2024 and March 2024, two providers of connected physical devices requested interoperability with a number of functionalities of iOS notifications, namely: (i) the ability to take an action in response to an iOS notification on a connected physical device, (ii) the ability to display images associated with an iOS notification on the connected physical device, (iii) the ability to display the app logo associated with an iOS notification on the connected physical device, and (iv) the ability to select which iOS notifications are sent to the connected physical device (the “iOS notifications feature”).¹²⁹
 - (b) In March 2024, one provider of connected physical devices requested interoperability with a number of functionalities of the high-bandwidth Wi-Fi-based peer-to-peer connection with an iPhone: (a) the ability to use the peer-to-peer connection while maintaining the iPhone’s existing Wi-Fi connections (so, e.g. initiation of the peer-to-peer connection does not cause the iPhone to lose internet access), (b) the ability to initiate peer-to-peer connections with the iPhone through a one-time user consent (e.g. the user is not required to manually open a device companion app and click a “join” prompt each time a connection is initiated), and (c) the ability to configure the iPhone (as opposed

¹²⁷ Judgment of 15 October 2014, *Parliament v Commission*, C-65/13, EU:C:2016:428, paragraphs 43-46 and the conclusions of Advocate General Cruz Villalón, in particular paragraphs 41- 42; judgment of 18 March 2014, *Commission v Parliament and Council*, C-427/12, EU:C:2014:170, paragraph 39.

¹²⁸ Judgment of 15 October 2014, *Parliament v Commission*, C-65/13, EU:C:2016:428, paragraph 44 and case law cited.

¹²⁹ Four requests submitted by [third-party developer] on 19 January 2024 through Apple’s “Feedback Assistant” system and one request submitted by [third-party developer] on 9 March 2024 through the Interoperability Request Portal.

to the wearable device) to serve as the Wi-Fi host (the “high-bandwidth peer-to-peer Wi-Fi connection feature”).¹³⁰

- (c) In January, March and April 2024, three providers of connected physical devices requested interoperability with the seamless proximity-based pairing feature, used to automatically start pairing and set-up of connected physical devices to the iPhone when brought in close proximity (the “proximity-triggered pairing feature”).¹³¹
- (d) In January 2024, one provider of connected physical devices requested interoperability with the continued and uninterrupted Bluetooth connection with an iPhone irrespective of whether the companion app of the connected physical device runs in the background of the iPhone (the “background execution feature”).¹³² Several other developers filed requests regarding background execution.
- (e) In October and November 2024, the Commission met with [...] providers of connected physical devices that expressed interest in interoperability with AirDrop and/or hardware and software features that enable third parties to develop a third-party iOS app for close-range wireless file transfers (the “features for close-range wireless file transfer solutions”).¹³³
- (f) In March 2024, one provider of connected physical devices requested interoperability with the feature that enables connected physical devices to have access to the Wi-Fi networks saved on a connected iOS device, without the need to re-enter the credentials on the connected physical device (the “automatic Wi-Fi connection feature”).¹³⁴
- (g) In March 2024, one provider of connected physical devices requested interoperability with Apple’s proprietary features for casting media between iOS devices and connected physical devices called AirPlay.¹³⁵ In addition, in November 2024, the Commission met with a provider of a casting solution, which indicated that Apple’s restrictions on casting solutions limit the ability for third-party media casting solutions to offer an experience competitive to AirPlay (the “features for media casting”).¹³⁶
- (h) In March and April 2024, two providers of connected physical devices requested interoperability with the feature to intelligently transfer audio

¹³⁰ One request submitted by [third-party developer] on 9 March 2024 through the Interoperability Request Portal.

¹³¹ One submitted by [third-party developer] on 19 January 2024 through Apple’s “Feedback Assistant” system, one submitted by [third-party developer] on 9 March 2024 through the Interoperability Request Portal and one submitted by [third-party developer] on 26 April through the Interoperability Request Portal.

¹³² One submitted by [third-party developer] on 19 January 2024 through Apple’s “Feedback Assistant” system.

¹³³ Agreed minutes of meeting with [third-party developer] of 24 October 2024; agreed minutes of meeting with [third-party developer] on 12 November 2024.

¹³⁴ One request submitted by [third-party developer] on 9 March 2024 through the Interoperability Request Portal.

¹³⁵ One request submitted by [third-party developer] on 9 March 2024 through the Interoperability Request Portal.

¹³⁶ Agreed minutes of meeting with [third-party developer] of 12 November 2024; [third-party developer]’s slide deck shared during the meeting with [third-party developer] on 12 November 2024.

between two audio sources connected to a connected physical device (e.g. a speaker or headphones) (the “automatic audio switching feature”).¹³⁷

- (i) In January and July 2024, two providers of connected physical devices requested interoperability with the feature to provision the secure element of a connected physical device (e.g. a wearable) with payment tokens through near field communication (“NFC”).¹³⁸ In February and October 2024, three providers of connected physical devices requested interoperability with the same feature to read bank card details for the purpose of verification of smart card possession in the context of secure customer authentication through NFC (the “NFC controller in reader/writer mode feature”).¹³⁹ In October 2024, two fashion companies contacted the Commission indicating that they are interested in offering products based on the NFC controller in reader/writer mode feature.¹⁴⁰
- (122) In April 2024, one provider of connected physical devices requested interoperability with the Spatial Audio feature, placing different sounds in different locations around the room.¹⁴¹ [...] ¹⁴² [...]
- (123) In the public consultation, respondents raised interoperability concerns in relation to several features that are not in the scope of these proceedings. This includes the following features.
 - (a) Number twinning. Apple enables number-twinning between the Apple Watch and iOS devices. This allows the Apple Watch to receive SMS messages and incoming calls even when it is not in range of the iOS device. Third-party connected physical devices do not have access to this feature.¹⁴³
 - (b) Synchronisation of system settings. Apple automatically synchronises settings such as “do not disturb” and alarms between iOS devices and the Apple Watch. This allows users a continuity of experience, as they do not have to enable such settings on each device separately. Third-party connected physical devices do not have access to this feature.¹⁴⁴
 - (c) Personal hotspot. Apple devices can seamlessly activate the personal hotspot of an iOS device, while for third-party devices the user must navigate through settings to connect.¹⁴⁵

¹³⁷ One submitted by [third-party developer] on 9 March 2024 through the Interoperability Request Portal and one submitted by [third-party developer] on 26 April through the Interoperability Request Portal.

¹³⁸ One submitted by [third-party developer] on 26 January 2024 through the Interoperability Request Portal and one submitted by [third-party developer] on 23 July 2024 through the Interoperability Request Portal.

¹³⁹ One submitted by [third-party developer] through the Interoperability Request Portal on 9 February 2024, one submitted by [third-party developer] on 14 October 2024 through the Interoperability Request Portal and two submitted by [third-party developer], one on 4 October 2024 through the Interoperability Request Portal and one on 15 October 2024 through the Interoperability Request Portal.

¹⁴⁰ Email from [third-party developer] of 16 October 2024 [on NFC access]; email from [third-party developer] of 16 October 2024 [on NFC access].

¹⁴¹ Interoperability request submitted by [third-party developer] through the Interoperability Request Portal on 26 April 2024.

¹⁴² [...]

¹⁴³ [Association]’s contribution to the public consultation.

¹⁴⁴ [Association]’s contribution to the public consultation.

¹⁴⁵ [Third-party developer]’s contribution to the public consultation.

- (d) Data back-up solutions. Third-party data back-up solutions face restrictions relating to synchronisation of data (e.g. background synchronisation) that iCloud does not have.¹⁴⁶
- (124) Since the opening of these specification proceedings, third parties have continued to submit requests for interoperability in Apple’s Interoperability Request Portal. These include the following requests related to connected physical devices.
- (a) In December 2024, a provider of a media streaming app submitted an interoperability request relating to media casting. The request comprises several media casting features, such as the possibility to adjust music volume with the physical buttons on the iPhone, populating the “Now Playing” widget on the lock screen and in the Control Centre, and keeping the streaming app and a network connection active while the app is in the background, so that the “Now Playing” widget can remain up to date.¹⁴⁷
 - (b) Several requests relate to access to the NFC controller in Reader/Writer mode such as the ability to read bank cards for enrolment and customer authentication in banking apps¹⁴⁸ and the possibility to transfer payment tokens via NFC.¹⁴⁹
 - (c) In October 2024, a car manufacturer submitted an interoperability request relating to Bluetooth Low Energy and ultra-wide band. The requester indicated that if users swipe away the app, the connection to the vehicle drops and the iPhone can no longer be used to unlock the vehicle.¹⁵⁰

5. MEASURES THAT THE COMMISSION IS SPECIFYING IN THIS DECISION

5.1. Overview of relevant features

- (125) The Decision is specifying measures that Apple needs to implement to effectively comply with Article 6(7) of Regulation (EU) 2022/1925 for the following features which are accessed or controlled via Apple’s operating system iOS and used by, and/or available to, Apple:
- (a) iOS notifications feature,
 - (b) high-bandwidth peer-to-peer Wi-Fi connection feature,
 - (c) proximity-triggered pairing feature,
 - (d) background execution feature,
 - (e) features for close-range wireless file transfer solutions,
 - (f) automatic Wi-Fi connection feature,
 - (g) features for media casting,
 - (h) automatic Bluetooth audio switching feature,

¹⁴⁶ [Third-party developer]’s contribution to the public consultation.

¹⁴⁷ Request by [third-party developer] on 16 December 2024 through the Interoperability Request Portal.

¹⁴⁸ Requests by [third-party developer] on 4 October 2024 and 15 October 2024 and [third-party developer] on 14 October 2024 through the Interoperability Request Portal.

¹⁴⁹ Request by [third-party developer] on 20 January 2025 and [third-party developer] on 1 October 2024 through the Interoperability Request Portal.

¹⁵⁰ Request by [third-party developer] on 29 October 2024 through the Interoperability Request Portal.

- (i) NFC controller in Reader/Writer mode feature.
- (126) Each of these features is further described below. Several features include or depend on certain functionalities, which may constitute features in their own right within the meaning of Regulation (EU) 2022/1925. The listed features and their description delineate the scope of the feature for the purpose of this Decision. Allowing interoperability with the same feature as is available to, or used by, Apple may thus require additional actions from Apple, including enabling various functionalities or access to other features for the purposes of granting effective interoperability with the features subject to this Decision.
- (127) This Decision specifies measures under Article 8(2) of Regulation (EU) 2022/1925 only for the specific features listed above. Several requests for other features relevant for third-party connected physical devices have been submitted to Apple's Interoperability Portal (see Section 1.3 of this Decision). These requested features, and any other iOS features relevant for third-party connected physical devices are outside the scope of this Decision. The Commission does not take a position as to whether these features are within the scope of Article 6(7) of Regulation (EU) 2022/1925 and whether Apple currently allows for effective interoperability with these features.
- (128) The Commission considers that the measures set out in this Decision, if implemented in practice, would be effective in achieving the objectives of Regulation (EU) 2022/1925 and of Article 6(7) of that Regulation and proportionate in the specific circumstances of the gatekeeper and the relevant service.
- (129) The presentation of the features reflects the situation in the most recent public release of iOS as of 10 December 2024, being iOS 18.1 released on 28 October 2024.¹⁵¹

5.2. Definitions

- (130) The following terms and technical concepts are used in this Decision.
- (131) "Application Programming Interfaces (APIs)" are software interfaces that allow two or more pieces of software to communicate with each other. APIs are typically implemented in one piece of software to offer (or 'expose') capabilities to other software, including applications. An API generally comes together with an API specification, i.e. a document describing how to use the API. The term API is sometimes used to refer to its specification, rather than its actual implementation.
- (132) "Frameworks" are reusable software building blocks, containing shared resources such as code and data.¹⁵² The Commission understands that frameworks are the primary unit in which iOS makes features available to third-party developers.¹⁵³ Frameworks offer APIs that provide a programmatic interface that apps call upon.¹⁵⁴

¹⁵¹ See <https://developer.apple.com/news/releases/?id=10282024a>, accessed on 5 November 2024.

¹⁵² See <https://developer.apple.com/library/archive/documentation/MacOSX/Conceptual/BPFrameworks/Concepts/WhatAreFrameworks.html>, accessed on 17 November 2024.

¹⁵³ Apple's developer documentation is primarily organised by framework, see <https://developer.apple.com/documentation>, accessed on 17 November 2024.

¹⁵⁴ See <https://developer.apple.com/documentation/xcode/diagnosing-memory-thread-and-crash-issues-early>: "Some system frameworks contain APIs [...]", accessed on 19 November 2024.

Apple's iOS SDK bundles these frameworks and APIs for use by third-party developers to build apps for iOS.¹⁵⁵

- (133) "Device discovery" refers to the ability of a device, whether it is an iPhone or a connected physical device, to discover or be discovered by nearby devices, e.g. by sending or listening to Bluetooth signals.¹⁵⁶ Device discovery may be automatic or may follow explicit user action.¹⁵⁷ Device discovery is essential in order to subsequently pair two devices and establish a connection between those devices.
- (134) "Pairing" refers to the process of connecting two nearby devices to establish a communication channel between the two devices. Nearby devices can typically be paired if they have either just discovered each other (see recital (135) of this Decision) or have a trusted relationship (see recital (133) of this Decision).¹⁵⁸
- (135) A "trusted device" is another device with which a device has a trusted relationship. Devices may establish a trusted relationship before or during the pairing process.¹⁵⁹
- (136) An "app" is an abbreviation for "software application" within the meaning of Article 2(15) of Regulation (EU) 2022/1925, defined there as any digital product or service that runs on an operating system.
- (137) An "iOS companion app" is an iOS app that facilitates the use of connected physical devices, such as the pairing between an iPhone and the connected physical device, setup of the connected physical device, controlling functionalities of the connected physical device, or offering services relating to the use of the connected physical device.¹⁶⁰
- (138) A "sister app" is an app that is designed to communicate with a corresponding app on another device.¹⁶¹ An iOS sister app is then an iOS app that is designed to

¹⁵⁵ See, for example, <https://developer.apple.com/documentation/ios-ipados-release-notes/ios-ipados-18-release-notes>; "The iOS & iPadOS 18 SDK provides support to develop apps for iPhone and iPad running iOS & iPadOS 18", accessed on 15 November 2024. See further, for example, <https://developer.apple.com/support/dma-and-apps-in-the-eu/>, accessed on 29 October 2024.

¹⁵⁶ In the case of Bluetooth, device discovery requires that the sending device is able to send advertisements, while the receiving device is able to constantly listen for and detect advertisements from nearby sending devices.

¹⁵⁷ For instance, proximity-triggered pairing depends on the automatic discovery of the nearby device, where the end user only needs to take action after the device has been discovered to continue pairing. In contrast, in order to connect speakers to an iPhone, the end user has to first take action by activating Bluetooth on both devices, before device discovery can occur and the speakers become visible in the list of available devices to which the iPhone can connect. See, for example, <https://support.apple.com/en-us/105108>, accessed on 21 February 2025.

¹⁵⁸ For instance, in the example referred to in recital (133) of this Decision, pairing the speaker to the iPhone is initiated once the end user clicks on the speaker on the list of available devices.

¹⁵⁹ If the nearby devices have no trusted relationship, the pairing process may require end users to exchange a (pre-shared) PIN or passcode before establishing a secure connection. Such an exchange may be manual – requiring the end user to insert the PIN – or automatic – for example, if the same end user signs into their personal account on both devices, or if the two devices belong to different end users who have each others' contact in their address book. If the nearby devices have a trusted relationship, the pairing process does not require the exchange of a PIN or passcode before establishing a secure connection.

¹⁶⁰ A companion app is usually developed and provided by the manufacturer of the connected physical device. The companion app usually acts as the primary link between an iPhone and a connected physical device, where both devices are possessed by the same user and are (eventually) paired.

¹⁶¹ Both apps are usually created by the same app developer (not necessarily the manufacturer of the connected physical device).

communicate with a corresponding app on a connected physical device. For instance, the user may install the same fitness app from an app developer both on the iOS device and a smartwatch, with the two apps being designed to transmit data to each other, for instance to keep fitness statistics synchronised.

- (139) “iOS Control Centre” is a menu that provides fast access to important functionalities on an iOS device, such as to quickly take a picture, turn on Wi-Fi, or control Apple TV. The user can access this menu at any time, regardless of the currently opened app. On iPhone X and later models, the menu can be opened by swiping down from the top-right corner of the screen.¹⁶²
- (140) “iOS settings” centralise the system-level configuration of preferences (“settings”) on iPhone, such as the user’s passcode and notification sounds.¹⁶³ iOS settings also enable control of certain settings that affect individual apps, for example app-by-app permissions to access certain information such as contacts, Bluetooth, or Local Network.¹⁶⁴
- (141) [...] ¹⁶⁵[...]

5.3. Measures for iOS notifications

- (142) Notifications are an essential feature of smartphones, including the iPhone. They are enabled by default and used by virtually all iPhone end users. One of the main benefits of owning a smartwatch (and other connected physical devices) is the ability to quickly view and react to notifications that the user has received on their smartphone, without having to reach out to their smartphone, unlock it, and react to the notification. The Apple Watch supports this integration with iOS notifications without restrictions. For example, if an iPhone user receives a photo from a friend, they can view the photo on their Apple Watch and they can send a reply message while just keeping the iPhone in their pocket. This is achieved thanks to Apple Watch’s privileged interoperability with the iPhone’s iOS notifications feature.
- (143) Third-party connected physical devices – including smartwatches – do not enjoy the same level of interoperability with this iOS feature. This means that third-party smartwatches do not have access to iOS notifications in the same way as the Apple Watch has, which prevents a level playing field.
- (144) Developers have requested interoperability with the iOS notifications feature for a long time and significantly before the submission of requests pursuant to Article 6(7) of Regulation (EU) 2022/1925. According to one developer, the wider developer community has been asking for interoperability with the iOS notifications feature since 2014.¹⁶⁶

5.3.1. Description of the feature

- (145) The iOS notifications feature consists in the ability to access, use, and transmit iOS notifications.
- (146) An iOS notification is a message, icon or another symbol that iOS displays or can display on an iPhone, by showing an alert, playing a sound, or badging the icon of an

¹⁶² See <https://support.apple.com/en-us/108330>, accessed on 21 February 2025.

¹⁶³ See <https://support.apple.com/en-ie/guide/iphone/iph079e1fe9d/ios>, accessed on 24 February 2025.

¹⁶⁴ See <https://support.apple.com/en-us/102515>, accessed on 24 February 2025.

¹⁶⁵ Apple’s reply to RFI 8 of 11 July 2024, question 1 and Annexes Q1b1-Q1b4.

¹⁶⁶ Technical meeting [third-party developer]/Commission on 2 May 2024, slide deck page 20.

app sending the iOS notification.¹⁶⁷ iOS notifications can be static or updated in real time (e.g. Live Activities). iOS notifications are an important means to draw end users' attention to Apple's and third-party apps' alerts and system events. Figure 1 below shows examples of iOS notifications as displayed on an iOS device.

Figure 1: iOS notifications shown on an iOS device



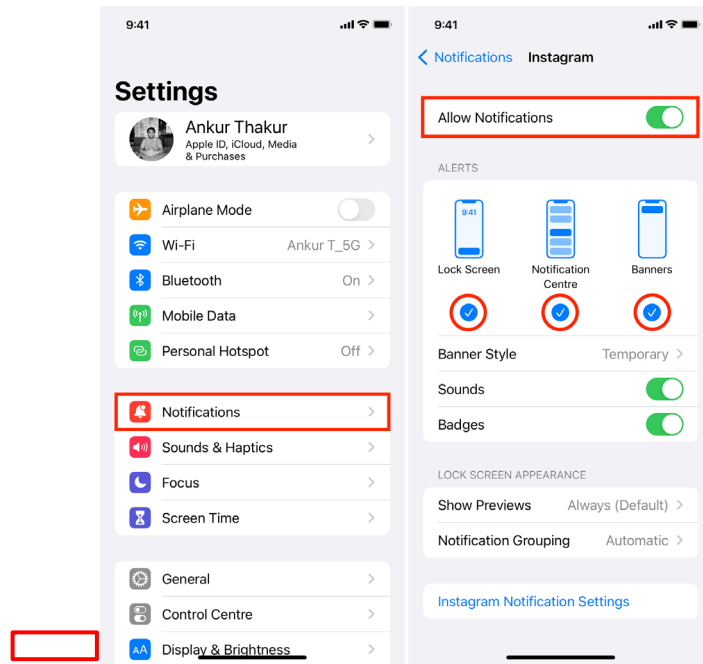
Source: <https://support.apple.com/en-us/108781>, accessed on 20 June 2024.

- (147) iOS notifications can originate from different sources, including the operating system iOS, Apple's apps and third-party apps. Before displaying iOS notifications for an app on an iPhone, Apple generally requires end users to explicitly grant permission for that app to submit iOS notifications. Usually, an end user is prompted to allow iOS notifications when using the respective app for the first time. Afterwards, users can configure (e.g. disable) notifications per app in the Notifications page of iOS settings (see Figure 2 below). Once an end user opts in for notification sourcing from a specific app, app developers can deliver iOS notifications to the end user's iPhone via iOS (as described in the next recital). iOS notifications are shown on the iPhone regardless of whether the app is actively running on the iPhone.¹⁶⁸

¹⁶⁷ See <https://developer.apple.com/documentation/usernotifications>, accessed on 20 June 2024.

¹⁶⁸ See <https://developer.apple.com/documentation/usernotifications>, accessed on 20 June 2024.

Figure 2: iOS notifications setting on an iOS device



Source: <https://www.idownloadblog.com/2015/05/25/how-to-apple-watch-instagram-notifications/>, accessed on 20 June 2024.

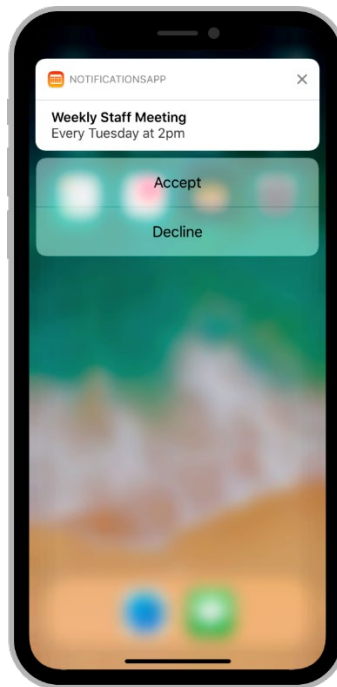
- (148) App developers can post iOS notifications via a so-called payload locally from the app or remotely from a server that they manage. The payload contains the custom iOS notification data including the delivery content and information about how iOS should notify the user. Local iOS notifications are generated locally on the iOS device by the app that runs on the device and delivered locally to the Notification Centre on the iPhone. For remote iOS notifications, the iOS app developer's server generates notifications and sends them to the Apple Push Notification service ("APNs"), which handles the delivery of those notifications to end users' connected physical devices.¹⁶⁹ APNs transmits the iOS notification directly to the end user's iPhone or connected physical device. If an iOS notification arrives while the device is switched on, but the app posting the iOS notification is not running, the system can still display the iOS notification. If the device is powered off when a notification is triggered, APNs will hold onto the notification and retry when the device is on again to deliver the notification.¹⁷⁰
- (149) iOS notifications include all notifications linked to an app developed for iOS, irrespective of whether they are locally generated by the iOS app on the iPhone or whether they are generated on the iOS app developer's server and transmitted through APNs. In the latter case, iOS notifications also include those notifications which are linked to an iOS app but sent directly from APNs to another Apple connected physical device (i.e. without passing through the iPhone).
- (150) When iOS displays an iOS notification on an iPhone, end users can tap it to see more options. The sender of the notification, e.g. a third-party app, can create actionable

¹⁶⁹ See <https://developer.apple.com/documentation/usernotifications>, accessed on 20 June 2024.

¹⁷⁰ See <https://www.airship.com/resources/explainer/ios-push-notifications-explained/#:~:text=If%20a%20notification%20arrives%20while,the%20device%20is%20on%20again>, accessed on 20 June 2024.

notifications which specify user options to react to the iOS notifications on iPhone such as reply to a message, call someone back, accept or decline a meeting invite, archive an email, and more. An example of an actionable notification is shown in Figure 3 below. Developers can define custom actions and notification types.¹⁷¹

Figure 3: Actionable notification on an iOS device



Source: <https://developer.apple.com/documentation/usernotifications/declaring-your-actionable-notification-types>, accessed on 20 June 2024.

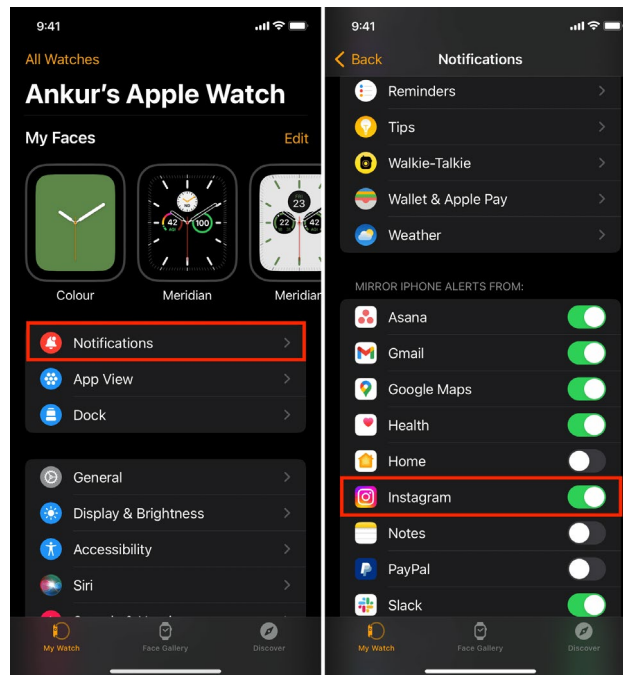
- (151) iOS allows developers to create rich notifications that contain supplementary content, such as visual and audio attachments as well as custom metadata to associate with the notification. These rich notifications are supported for both locally and remotely generated notifications.¹⁷²
- (152) Apple's smartwatch, the Apple Watch, can fully mirror iOS notifications and their respective functionalities available on the iPhone. End users can therefore receive, see, and interact with iOS notifications on the Apple Watch as they can on the iPhone.
- (153) End users can choose which, if any, iOS notifications are displayed on the Apple Watch through the Watch app on the paired iPhone and how (e.g. whether to allow sound, whether they appear on the lock screen). End users can change notification settings for the Apple Watch for all apps, or separately for each app (see Figure 4 below). End users can manage where notifications appear on the Apple Watch, can mute notifications (e.g. for 1 hour) or turn them off. Some apps allow an end user to

¹⁷¹ See <https://developer.apple.com/documentation/usernotifications/declaring-your-actionable-notification-types>, accessed on 20 June 2024.

¹⁷² For local notifications, see section "Providing supplementary content" at <https://developer.apple.com/documentation/usernotifications/unmutablenotificationcontent>, accessed on 20 June 2024. For remote notifications, see section "Providing supplementary content" at <https://developer.apple.com/documentation/usernotifications/unnotificationcontent>, accessed on 20 June 2024.

customize their notifications further, which end users can do in the settings menu of the Watch app.¹⁷³

Figure 4: iOS notification settings for the Apple Watch in the Watch app



Source: <https://www.idownloadblog.com/2015/05/25/how-to-apple-watch-instagram-notifications/>, accessed on 20 June 2024.

- (154) The functionalities of the iOS notifications feature available to the Apple Watch include, amongst others, the following functionalities.¹⁷⁴
- (a) Forward notifications. iOS notifications are forwarded to and displayed on the Apple Watch. Instead of appearing both on the iPhone and on the Apple Watch, iOS notifications appear only on the device that is most likely to have the user's current focus. This depends on the notification type, the process that created the notification (i.e. whether it is generated locally, remotely or in the background), and the currently active device. [...] ¹⁷⁵
 - (b) Actionable notifications. For actionable notifications described in recital (150) of this Decision, the Apple Watch allows for the same actions in reply to an iOS notification as the iPhone. End users can therefore interact directly from the notification's interface on the Apple Watch and undertake app-specific actions (e.g. notifications can be dismissed, users can reply to a message, call someone back, archive an email). If any of these actions are undertaken on the Apple Watch, the action is mirrored on the iPhone as well. For example, if an end user accepts a meeting invitation on the Apple Watch, the invite will also appear as accepted on the iPhone.
 - (c) Rich notifications. In reference to rich notifications on iOS (see recital (151) of this Decision), iOS Notifications on Apple Watch can carry attachments (e.g.

¹⁷³ See <https://support.apple.com/guide/watch/change-notification-settings-apd9b833c9f3/watchos>, accessed on 30 October 2024.

¹⁷⁴ Apple's reply to RFI 1 of 23 September 2024, question 7.

¹⁷⁵ Apple's reply to RFI 1 of 23 September 2024, question 3.

media assets with a thumbnail preview)¹⁷⁶ and metadata (e.g. the posting app’s notification icons).¹⁷⁷ Figure 5 below shows an example of a rich and actionable Instagram iOS notification as displayed on the Apple Watch with the app logo, an associated image and the ability to “like” the iOS notification, i.e. respond to it.

Figure 5: Example of a rich and actionable iOS notification on the Apple Watch



Source: <https://www.idownloadblog.com/2015/05/25/how-to-apple-watch-instagram-notifications/>, accessed on 20 June 2024.

- (d) Notification settings. In the companion app of the Apple Watch, end users can individually decide whether the iOS notifications of a certain app are mirrored on the Apple Watch (see Figure 4 of this Decision). End users can also decide that no iOS notifications are sen[t] to the Apple Watch at all (while they are still being shown on the iOS device).
 - (e) Priority Notifications and Notification Summaries. Apple recently rolled out two new functionalities for iOS notifications: Priority Notifications and Notification Summaries.¹⁷⁸ The Priority Notifications functionality displays notifications which are marked as a priority at the top of the iOS lock screen ensuring immediate visibility. The Notification Summaries functionality allows users to receive a summary of non-emergency notifications at scheduled times. Users are or will be able to access both functionalities on the Apple Watch.¹⁷⁹
- (155) iOS notifications are not only available to the Apple Watch, but also to Apple’s augmented reality headset Apple Vision Pro.¹⁸⁰ For example, end users can decide

¹⁷⁶ [...]

¹⁷⁷ [...]

¹⁷⁸ Both functionalities were not available at the time of the opening of these proceedings, i.e. on 19 September 2024. However, Apple released both functionalities for iOS 18.1 in October 2024 in certain parts of the world (see <https://www.apple.com/newsroom/2024/10/apple-intelligence-is-available-today-on-iphone-ipad-and-mac/>, accessed on 4 February 2025). In the EU, Apple has made available both functionalities for testing in February 2025 (see Apple’s email of 17 February 2025 [...]).

¹⁷⁹ See, for example, <https://9to5mac.com/apple-watch-will-get-key-apple-intelligence-feature-in-ios-18-1/>, accessed on 20 June 2024.

¹⁸⁰ See <https://support.apple.com/nl-be/guide/apple-vision-pro/tan3c28cb971/visionos>, accessed on 20 October 2024.

which apps can send iOS notifications to the Apple Vision Pro and can change how notifications appear.¹⁸¹

5.3.2. *Feature falls within the scope of Article 6(7) of Regulation (EU) 2022/1925*

- (156) The Commission finds that the iOS notifications feature as described in Section 5.3.1 of this Decision – together with its functionalities – falls within the scope of Article 6(7) of Regulation (EU) 2022/1925. iOS notifications are a software feature which is controlled via iOS, Apple’s operating systems for iPhones, which is listed in the Designation Decision.

5.3.3. *Current implementation for Apple’s own services and hardware*

- (157) The iOS notifications feature is available to and used by Apple. Indeed, Apple’s own connected physical devices, such as the Apple Watch or Apple Vision Pro, benefit from the full range of iOS notifications functionalities: they can access and receive iOS notifications and their metadata via different data transports, depending on whether the Apple Watch is in the iPhone’s proximity. If an Apple Watch is near the iPhone, the iPhone will send iOS notifications to the Apple Watch over Bluetooth. If an Apple Watch is outside the range of Bluetooth, iOS notifications may be sent to the Apple Watch over the local Wi-Fi network or via an independent cellular connection relying on APNs.¹⁸² The iOS notifications feature is also available to Apple’s augmented reality headset Apple Vision Pro, as explained in recital (155) of this Decision.¹⁸³

5.3.4. *Current implementation for third-party services and hardware*

- (158) Third-party connected physical devices, including third-party smartwatches, can receive notifications from Apple and third-party apps that appear in the iPhone’s Notification Centre via the Apple Notification Center Service (“ANCS”). ANCS relies on a [Bluetooth Low Energy (“BLE”)] connection between the iPhone and the third-party connected physical device. Apple’s own connected physical devices, including Apple Watch, do not use ANCS.
- (159) ANCS allows for the forwarding of text-only notifications. iOS notifications forwarded over ANCS include the app identifier, title, subtitle, message body and date. According to Apple, ANCS was developed primarily as an ‘outbound’ tool that allows the display of iOS notifications on a connected physical device but not the sending of replies to iOS notifications from the connected physical device to the iOS device. Interaction with ANCS notifications on the third-party connected physical device allow a single “positive action” and “negative action,” for example accepting or declining an incoming call.¹⁸⁴
- (160) A number of iOS notifications functionalities available to or used by the Apple Watch are not currently available to third-party connected physical devices. Indeed, according to Apple,¹⁸⁵ ANCS does not provide third-party connected physical devices with several functionalities of the iOS notifications feature which are

¹⁸¹ See <https://support.apple.com/nl-be/guide/apple-vision-pro/tanc26d9edb9/visionos>, accessed on 20 October 2024.

¹⁸² Apple’s reply to RFI 1 of 23 September 2024, question 3.

¹⁸³ See <https://support.apple.com/nl-be/guide/apple-vision-pro/tan3c28cb971/visionos>, accessed on 20 October 2024.

¹⁸⁴ Apple’s reply to RFI 1 of 23 September 2024, question 7.

¹⁸⁵ Apple’s reply to RFI 1 of 23 September 2024, question 7.

available on Apple’s connected physical devices. *First*, ANCS does not support “actionable notifications.” Notifications proxied via ANCS do not allow for actions such as accepting or declining a calendar invite, replying to messages or custom actions, e.g. liking a social media post. *Second*, ANCS does not support “rich notifications,” meaning ANCS does not allow for a notification to carry attachments, thumbnails previews or other metadata. *Third*, [...]. *Fourth*, ANCS does not allow users to choose which apps can send iOS notifications to the connected physical device. ANCS also does not allow for a system-wide dismissal of the sending of iOS notifications to the connected physical device. Instead, the user’s settings for the display of notifications on the iPhone automatically apply to the connected physical device. Therefore, a user can only disable or enable notifications for both devices (the iPhone and connected physical device) but not individually. *Lastly*, ANCS only supports Bluetooth as a transport technology and no other wireless technologies such as Wi-Fi or cellular.

- (161) The developer documentation for ANCS on Apple’s website was last updated on 20 October 2014, i.e. a few months before the release of the first Apple Watch in April 2015. According to Apple, only minor functionalities (user alerts and call controls) were added to ANCS following the release of the Apple Watch.¹⁸⁶
- (162) Apple explained that, besides ANCS, it allows third-party connected physical devices to build a customised data pipeline with a companion app on iOS. That data pipeline allows a developer to forward its own notifications to the third-party connected physical device.¹⁸⁷ These notifications can be actionable and can carry attachments and/or metadata, at the developer’s discretion. However, such solution only works for notifications of the companion app itself but not for notifications of any other Apple or third-party app.
- (163) iOS also appears to support the so-called Bluetooth Messaging Access Profile (“Bluetooth MAP”). Bluetooth MAP can be used, to some extent, for the transmission of iOS notifications to a connected physical device. However, Bluetooth MAP does not support the BLE standard used by the Apple Watch. Instead, it relies on the older so-called Bluetooth Classic transmission technology. Bluetooth Classic consumes significantly more power than BLE. The industry is therefore transitioning away from Bluetooth Classic to BLE and newer connected physical devices do not support Bluetooth Classic anymore.¹⁸⁸
- (164) Therefore, the Commission considers that there is currently an interoperability gap when it comes to third-party connected physical devices connected to iOS devices and that it should specify how Apple has to fill this gap to comply with Article 6(7) of Regulation (EU) 2022/1925.

5.3.5. *The gatekeeper’s view*

- (165) Apple does not seem to contest that Article 6(7) of Regulation (EU) 2022/1925 requires it to provide interoperability with iOS notifications as such.¹⁸⁹ However, Apple argues that an obligation to provide interoperability with future updates, including new functionalities, of the iOS notifications feature goes beyond what is legally required for providing effective interoperability with the iOS notifications

¹⁸⁶ Apple’s reply to RFI 1 of 23 September 2024, question 4.

¹⁸⁷ Apple’s reply to RFI 1 of 23 September 2024, question 1.

¹⁸⁸ [Third-party developer]’s reply to RFI 1 of 13 June 2024, Annex 1.

¹⁸⁹ Apple’s reply to the Preliminary Findings, Section VII.A.

feature and would interfere with Apple's fundamental rights. According to Apple, such a requirement to provide interoperability with future updates would reduce Apple's incentives to innovate, increase costs, undermine Apple's market differentiation, delay product launches and allow third parties to free ride on Apple's proprietary innovations.¹⁹⁰

(166) Apple claims that the Commission's Preliminary Findings are based on insufficient and non-representative evidence and do not sufficiently assess the effectiveness of Apple's current interoperability solution or the importance of the functionalities of the iOS notifications and their impact on contestability.¹⁹¹

(167) [...] ¹⁹²

(168) [...] ¹⁹³ [...] ¹⁹⁴

5.3.6. Commission's assessment

(169) Apple appears to agree that it should provide interoperability with the iOS notifications feature. [...] ¹⁹⁵

(170) As described in Section 3.1.3 of this Decision, Apple also needs to allow for interoperability with any future updates, including new functionalities, of the iOS notifications feature insofar they are available to Apple. The language and aim of Article 6(7) of Regulation (EU) 2022/1925 do not foresee any delay of interoperability solutions. Timely interoperability is crucial for developers of connected physical devices to be able to effectively compete with Apple and limit Apple's inherent first-mover advantage and entrenched market position. As detailed in Section 3.1.3 of this Decision, this does not reduce Apple's incentives to innovate or deprive Apple of its competitive advantage. Apple benefits, for example, from Summary Notifications and Priority Notifications on iOS and had more time than any competing provider of connected physical devices to adapt its own services and hardware, for example the Apple Watch, to these new functionalities of the iOS notifications feature.

(171) Importantly, it is not for Apple or the Commission to decide which features or functionalities are relevant or important enough to justify an interoperability solution. *First*, Article 6(7) of Regulation (EU) 2022/1925 simply requires interoperability with the same features as available to Apple under equal conditions. *Second*, the iOS notifications feature is subject of four individual requests by one developer who considers it commercially very important.¹⁹⁶ *Third*, the ability to respond to notifications, e.g. new messages or app alerts, directly from a smartwatch is one of

¹⁹⁰ Apple's reply to the Preliminary Findings, paragraph 120.

¹⁹¹ Apple's reply to the Preliminary Findings, paragraphs 127 and 128.

¹⁹² Email from Apple to the Commission on 17 February 2025 [on the draft final measures].

¹⁹³ Apple's reply to the Preliminary Findings, paragraphs 121 and 126.

¹⁹⁴ Email from Apple to the Commission of 3 February 2025 [...]; Email from Apple to the Commission of 17 February 2025 [on the draft final measures].

¹⁹⁵ Apple's internal document submitted in response to RFI by decision of 26 September 2024 (Commission Decision C(2024) 6879 final) and amended on 14 October 2024 (Commission Decision C(2024) 7318 final) ("Apple's internal document") [...].

¹⁹⁶ Apple's reply to the Preliminary Findings, paragraph 119; Email from Apple to the Commission of 17 February 2025 [on the draft final measures].

the top considerations for smartwatch purchasers – and one of the most used product features when it is available. [...] ¹⁹⁷ [...] ¹⁹⁸

- (172) With regards to Apple’s concerns regarding the access to iOS notifications data by third-party developers for purposes other than the pre-processing of iOS notifications for the transmission to a connected physical device, the following aspects have to be considered. *First*, enabling the pre-processing of iOS notifications is crucial so that third-party developers can determine and optimise how the iOS notification is relayed to the connected physical device, and thus optimise the user experience. They might, for example, adapt the size of an image of the iOS notification or summarise the content of the iOS notification depending on the capabilities of the respective connected physical device. Apple, for example, uses pre-processing of notifications to provide notification summaries on Apple devices and notification announcements on AirPods. ¹⁹⁹ *Second*, this Decision and its measures focus on interoperability for connected physical devices. The aim of the measures for the iOS notifications feature is to enable third-party connected physical devices to receive, access, use, and respond to iOS notifications. Consequently, the measures under this Decision pertain to use cases for connected physical devices. *Third*, when accessing and processing iOS notifications data, for example for user profiling, third parties remain subject to applicable legislation, including the “purpose limitation” and transparency obligations of Regulation (EU) 2016/679 (GDPR). ²⁰⁰ Therefore, for the purposes of these proceedings, it is not necessary to decide whether Apple may restrict the use of the iOS notification data as proposed.
- (173) Apple argued that this measure would prevent it from mandating end-to-end encryption, i.e. that the notification stays encrypted between iOS and the connected device. ²⁰¹ This is incorrect: the measure allows Apple to precisely require that the notification is encrypted before sending it to the connected device. This means that notifications would always be encrypted in transit.
- (174) The Commission also notes that Apple uses the expression “end-to-end encryption” to refer to encryption “between iOS and the connected device”, i.e. encryption in transit. However, in fact, iOS notifications are already decrypted in iOS. This also reflects the most common behaviour for the Apple Watch, where even for popular end-to-end encrypted messaging apps like Signal or Telegram, the content is decrypted on iOS prior to re-encryption on iOS and forwarding to the Apple Watch. ²⁰² In any case, as described, Apple can require this type of encryption.
- (175) Finally, as regards timing, it is important that Apple implements the iOS notifications features as soon as possible. Apple has used for its own services and hardware most of the functionalities of the iOS notifications feature for several years, meaning that these functionalities are well established and known. Apple has had a significant amount of time to consider and work on an interoperability solution for the iOS notifications feature. Apple received the first formal requests for interoperability with

¹⁹⁷ See, for example, antitrust complaint filed against Apple by the United States Department of Justice on 21 March 2024, paragraph 101.

¹⁹⁸ Apple’s internal document [...].

¹⁹⁹ [Third-party developer]’s submission of 29 January 2025 paragraph 2.5.2.

²⁰⁰ OJ L 119, 4.5.2016, pages 1-88.

²⁰¹ Email from Apple to the Commission on 17 February 2025 [on the draft final measures].

²⁰² Apple’s reply to RFI 3 of 7 October 2024, question 31.

iOS notifications in January 2024. [...] ²⁰³ The wider developer community has been asking for interoperability with iOS notifications since 2014. ²⁰⁴ A third party considered the level of work required from Apple as “low.” ²⁰⁵ [...] ²⁰⁶

- (176) [...] ²⁰⁷ Taking into account these realities and the importance of a complete, stable and well-functioning interoperability solution, the implementation timing proposed by Apple seems to be the most appropriate way forward. The Commission does maintain that Apple could have and should have started working on the implementation of the iOS notifications feature earlier pursuant to the principles described in Section 3.1 of this Decision.

5.3.7. *Measures that Apple should implement*

- (177) To meet the requirements of Article 6(7) of Regulation (EU) 2022/1925, Apple should implement an interoperability solution that provides third parties with access to the same iOS notifications feature as available to Apple (as described in Section 5.3.1 of this Decision), in a way that is equally effective as the solution available to Apple.
- (178) Apple should provide effective interoperability with all functionalities of the iOS notifications feature which are available to Apple’s own connected physical devices, including, but not limited to, AirPods, Apple Watch, Apple Vision Pro, as well as any future Apple connected physical devices. These functionalities are:
- (179) receiving iOS notifications on the connected physical device and taking actions in response to iOS notifications, including custom actions defined by the third-party developer, on the connected physical device to ensure that the response or interaction is registered and reflected by the iOS device;
- (a) selecting which iOS notifications are shown on each connected physical device within the companion app of the respective connected physical device or iOS settings, at the developer’s option; and
 - (b) displaying logos associated with the app posting the iOS notification and images, attachments and other metadata associated with the iOS notification on the connected physical device.
- (180) Apple should grant third parties access to additional functionalities if necessary to enable effective interoperability with the iOS notifications feature described in Section 5.3.1 of this Decision. ²⁰⁸
- (181) To provide third parties with an interoperability solution for the iOS notifications feature described in Section 5.3.1 of this Decision that is equally effective as that available to any of Apple’s own connected physical devices, Apple should implement the following measures.

²⁰³ Apple’s internal document [...].

²⁰⁴ Technical meeting [third-party developer]/Commission of 2 May 2024, slide deck page 20.

²⁰⁵ [Third-party developer]’s reply to RFI 1 of 13 June 2024, Annex 1.

²⁰⁶ Apple’s internal document [...].

²⁰⁷ [...] and email from Apple to the Commission of 17 February 2025 [on the draft final measures].

²⁰⁸ This requirement aims to ensure that Apple makes all relevant capabilities available to third parties necessary to enable effective interoperability with the iOS notifications feature. The Commission and third parties may not be aware of all capabilities due to the technical complexity, limited transparency and changing nature of an operating system such as iOS. This requirement applies *mutadis mutandis* to all other features within the scope of this Decision for the same reasons. [...]

- (a) Apple should provide third-party iOS apps, in particular companion apps of connected physical devices, with the full and complete payload and metadata²⁰⁹ of all iOS notifications. The third party and the end user must then be able to decide whether and how an iOS notification is relayed to the third-party connected physical device. To ensure interoperability under equal conditions with Apple's connected physical devices, Apple should ensure that the third party is able to pre-process in its iOS app the iOS notifications, for example to adjust the size of an image or summarise a text, before the iOS notification is relayed to the third-party connected physical device.²¹⁰ Apple is allowed to require that third-party developers encrypt the iOS notification before relaying it to the connected physical device.
 - (b) Apple should ensure that third parties are free to decide which transport technology they want to use to relay the iOS notification to the connected physical device (e.g. Bluetooth only or other technologies such as infrastructure Wi-Fi, peer-to-peer Wi-Fi or cellular connections).
 - (c) Apple should allow third parties to implement in their iOS app, or Apple should make available in iOS settings, at the developer's option, functionality which enables end users to decide which iOS notifications from which apps are relayed to the third-party connected physical device.²¹¹ Apple should also allow third parties to implement in their iOS app functionality which enables end users to decide whether iOS notifications from a given app should be shown or not shown at certain times or under certain conditions (e.g. during certain activities or times of the day).
- (182) Apple should ensure that any interoperability solution for iOS notifications does not require any changes or further implementation to apps posting iOS notifications.²¹² To the extent the developer of an app sending iOS notifications has enabled certain functionalities or settings for the relay and showing of its iOS notifications on Apple's connected physical devices, in particular the Apple Watch, these must automatically and to the same extent be available to third parties.²¹³
- (183) Apple should also provide effective interoperability with any future updates, including new functionalities, of the iOS notifications feature insofar as they are

²⁰⁹ Enabling, for example, the display of logos associated with the app posting the iOS notification as well as images and attachments associated with the iOS notification on the connected physical device.

²¹⁰ Allowing such pre-processing of iOS notifications is crucial for developers to determine and optimise how the notification is relayed to the connected physical device. Apple, for example, uses pre-processing of notifications to provide notification summaries on Apple devices and notification announcements on AirPods. See [third-party developer]'s submission of 29 January 2025, paragraph 2.5.2.

²¹¹ It is critical for developers to be able to implement such a settings menu for iOS notifications in their companion app. Only such an option will ensure a frictionless user journey, avoiding the need for a user to switch between the iOS settings and the companion app – see also recital (88) of this Decision. Apple has implemented such a settings menu, for example, in the Apple Watch companion app. See [third-party developer]'s submission of 29 January 2025, paragraph 2.5.3.

²¹² Neither from developers of apps posting iOS notifications or of their end users. In particular, Apple may not require developers to change or add the programming of the payload of their iOS notifications.

²¹³ For example, if a messaging app developer has defined certain parameters for the showing of its iOS notifications – such as the headline, icon, or playing a sound – the same notification with the same parameters must be available out-of-the-box to third-party smartwatches, without the need for the messaging app developer to make special changes to their app in order to support third-party connected physical devices.

available to Apple's own connected physical devices. To this end, the general measures in Section 5.12 of this Decision apply, including in particular the measures concerning future updates and new functionalities set out in Section 5.12.7 in this Decision. To the current knowledge of the Commission, future or recently introduced updates of the iOS notifications feature include:

- (a) prioritising certain notifications on top of the screen of the connected physical device (so called "Priority Notifications"); and
- (b) showing a summary of non-emergency notification at scheduled times (so called "Summary Notifications").

(184) Apple should implement the measures above in compliance with the measures for all features in Section 5.12 of this Decision.

5.3.8. *Implementation timing*

(185) Following Apple's own proposal and estimate, Apple should implement the measures for the iOS notifications feature (except for (i) the ability to select which iOS notifications are shown on each connected physical device within the companion app, and (ii) the functionalities described in recital (183) of this Decision) in a beta version of iOS available to developers by the end of 2025 at the latest. Apple should thereafter implement all measures for the iOS notifications feature by 1 June 2026 at the latest.

5.4. **Measures for High-Bandwidth Peer-to-Peer Wi-Fi Connection**

(186) Several modern iOS features rely on high-bandwidth peer-to-peer ("P2P") Wi-Fi connections (hereinafter referred to as "P2P Wi-Fi connection feature"). This type of connection allows Apple services and hardware to exchange content with an iPhone quickly and without depending on external networks or hardware. For example, iPhone users can quickly send a video to their Apple Vision Pro while they are on a train, without the need to connect either the iPhone and the Apple Vision Pro to the train's Wi-Fi or to a cellular network. Similarly, iPhone users can use their iPhone as an external camera for their Mac computer wherever they are, without the need to use a cable or have a shared Wi-Fi network available. Apple's ability to provide these functionalities on its connected physical devices relies on privileged interoperability with iOS, which allows it to initiate and control high-bandwidth P2P Wi-Fi connections.

(187) Third parties are not able to provide a comparable user experience, despite their best efforts, in part because they cannot access the same iOS features. Moreover, they are unable to provide new, innovative services that would be possible by using such versatile, fast, and easy-to-use Wi-Fi connections. The Commission notes that access to high-bandwidth P2P Wi-Fi alone may not be sufficient to enable some use cases that may rely on additional iOS features too (see, for instance, Sections 5.7 and 5.9 of this Decision). However, high-bandwidth P2P Wi-Fi is often an important component needed to provide the same user experience as Apple's connected physical devices.

(188) Developers have requested interoperability with the P2P Wi-Fi Connection feature for a long time and significantly before the submission of requests pursuant to Article 6(7) of Regulation (EU) 2022/1925. According to a third party, the wider developer

community has been asking for interoperability with the P2P Wi-Fi connection feature since 2016.²¹⁴

5.4.1. *Description of the feature*

- (189) The P2P Wi-Fi connection feature consists in the ability to establish and use a high-bandwidth Wi-Fi connection between an iOS device and a connected physical device.
- (190) iOS devices are capable of establishing a high-bandwidth P2P Wi-Fi connection with another Apple device, such as an Apple Watch, Apple Vision Pro, iPhone or Mac, in order to transfer data across devices. The data connection is referred to as a “P2P” Wi-Fi connection as the devices connect without an intermediary. This means that the P2P Wi-Fi connection feature can transfer data across devices independently of whether the involved devices are connected to any local infrastructure Wi-Fi or cellular network.
- (191) Apple currently uses two communication protocols to implement a P2P Wi-Fi connection, namely Apple Wireless Direct Link (“AWDL”) and Wi-Fi Aware (see Section 5.4.3 of this Decision).
- (192) iOS devices can establish a P2P Wi-Fi connection with an Apple connected physical device that supports the same P2P Wi-Fi communication protocol. iOS devices cannot establish a P2P Wi-Fi connection with third-party connected physical devices through either of the two connection protocols, as Apple has neither made AWDL available to third-party hardware providers,²¹⁵ nor made Wi-Fi Aware available to third-party iOS developers.²¹⁶
- (193) The P2P Wi-Fi connection feature is used by Apple for numerous purposes and across different devices to quickly transfer large amount of data across two devices. For instance, Apple uses P2P Wi-Fi connections on iOS devices to transfer files or photos to an Apple connected physical device via AirDrop,²¹⁷ mirroring video content to an Apple connected physical device via AirPlay,²¹⁸ [...] ²¹⁹ [...] ²²⁰
- (194) iOS devices are capable of channel switching. Channel switching allows iOS devices to maintain a P2P Wi-Fi connection with connected physical devices independently and concurrently to maintaining an infrastructure Wi-Fi connection providing internet access.²²¹ [...] ²²² [...]
- (195) The ability of channel switching has several advantages for users of connected physical devices. For example, a connected physical device can establish both, a P2P Wi-Fi connection with the iOS device to send or receive data between two devices, while at the same time using an internet connection of the iOS device if the connected physical device cannot establish its own infrastructure Wi-Fi or cellular

²¹⁴ Technical meeting [third-party developer]/Commission of 2 May 2024, slide deck page 18.

²¹⁵ Apple’s reply to RFI 1 of 23 September 2024, question 19.

²¹⁶ Technical meeting [third-party developer]/Commission of 12 November 2024, slide deck page 6.

²¹⁷ See https://help.apple.com/pdf/security/en_GB/apple-platform-security-guide-b.pdf, page 186, accessed on 8 October 2024.

²¹⁸ See https://help.apple.com/pdf/security/en_GB/apple-platform-security-guide-b.pdf, page 186, accessed on 8 October 2024.

²¹⁹ Apple’s reply to RFI 1 of 23 September 2024, question 15 and Table 1.

²²⁰ Apple’s reply to RFI 3 of 7 October 2024, question 1.

²²¹ Apple’s reply to RFI 1 of 23 September 2024, question 18.

²²² Technical meeting Apple/Commission of 3 October 2024, slide deck pages 7 and 9.

network connection (e.g. to update apps on the connected physical device via the iOS companion app). For this purpose, the iOS device should be able to maintain an infrastructure Wi-Fi connection such that it can connect to the internet, while simultaneously remaining connected with the connected physical device via the P2P Wi-Fi connection. Furthermore, a P2P Wi-Fi connection consumes less battery power than establishing a direct connection to the internet via the connected physical device.²²³

(196) Further functionalities of the P2P Wi-Fi connection feature available to Apple services or hardware are:

- (a) initiating a P2P Wi-Fi connection by discovering nearby connected physical devices and securely pairing with a nearby connected physical device via P2P Wi-Fi;
- (b) establishing a P2P Wi-Fi connection with high bandwidth, high speed, and latency, that does not have a central coordinator, and that can be maintained for the same amount of time as is available to Apple;²²⁴
- (c) establishing a P2P Wi-Fi connection that can run independently and concurrently to infrastructure Wi-Fi (e.g. via internet router or, if Apple makes such a hotspot available to any of its own connected physical devices, hotspot provided by the iOS device or connected physical device) via channel switching, as well as synchronization to improve the performance of channel switching;²²⁵
- (d) establishing a P2P Wi-Fi connection that serves as a hotspot providing internet access to a connected physical device using a concurrent connection (e.g. cellular), if Apple makes such a functionality available to any of its own connected physical devices;²²⁶
- (e) establishing multiple concurrent P2P Wi-Fi connections without discontinuing existing P2P Wi-Fi connections between an iOS device and connected physical devices;²²⁷
- (f) establishing a P2P Wi-Fi connection upon request of the relevant third-party iOS app, without further user intervention via the companion app or otherwise, or without more user intervention than is required between Apple devices to establish a P2P Wi-Fi connection;²²⁸
- (g) allowing the P2P Wi-Fi connection between trusted devices to run in the background after initiation, without the need for the app(s) initiating the P2P Wi-Fi connection to be in the foreground;²²⁹
- (h) once established, allowing iOS apps to use the P2P Wi-Fi connection, to access the same connection metadata,²³⁰ and to allow third parties to configure the

²²³ [Third-party developer]’s reply to RFI 1 of [Confidential], question 8.

²²⁴ Technical meeting Apple/Commission of 3 October 2024, slide deck page 12; [third-party developer]’s contribution to the public consultation.

²²⁵ Technical meeting Apple/Commission of 3 October 2024, slide deck page 6; Apple’s reply to RFI 3 of 7 October 2024, question 11.

²²⁶ [...].

²²⁷ Apple’s submission of 7 November 2024, page 3, Table 1.

²²⁸ [Third-party developer]’s reply to RFI 1 of [Confidential], question 8.

²²⁹ [Third-party developer]’s reply to RFI 1 of [Confidential], question 7.

same parameters²³¹ of the Wi-Fi Aware connection as Apple uses itself in its P2P Wi-Fi connection solution;

- (i) disabling the P2P Wi-Fi connection automatically once the use case is completed in order to save battery power and Wi-Fi bandwidth.

(197) Further functionalities of the P2P Wi-Fi connection feature will be available to Apple’s own connected physical devices in the future. These future functionalities include, among others:

(a) [...] ²³²

(b) [...] ²³³

5.4.2. *Feature falls within the scope of Article 6(7) of Regulation (EU) 2022/1925*

(198) The Commission finds that P2P Wi-Fi connection as described in Section 5.4.1 of this Decision – including the functionalities described in that section– falls within the scope of Article 6(7) of Regulation (EU) 2022/1925. The P2P Wi-Fi connection is a hardware and software feature which is controlled via iOS, Apple’s operating systems for iPhones, which is listed in the Designation Decision.

5.4.3. *Current implementation for Apple’s own services and hardware*

(199) The P2P Wi-Fi connection feature is available to and used by Apple. Apple’s own connected physical devices, such as the iPhone, iPad, Apple Watch, or Apple Vision Pro, can establish a P2P Wi-Fi connection in two ways. Apple devices can use Apple’s proprietary AWDL protocol or the Wi-Fi Aware protocol.²³⁴

(200) AWDL and Wi-Fi Aware are different P2P Wi-Fi communication protocols. Both protocols allow for a low latency high-speed P2P Wi-Fi connection with no central coordinator. However, the Commission understands that Wi-Fi Aware, and in particular version 4.0 of its specification, supports newer, faster Wi-Fi technologies, has built-in pairing, security, and privacy protections, and has industry certification and interoperability programs as an open and public standard.²³⁵

(201) Since 2012, Apple worked with participants of the standardising body Wi-Fi Alliance to standardise a Neighbour Awareness Networking (“NAN”) protocol that establishes a P2P Wi-Fi connection.²³⁶ Whereas Apple initially proposed to standardise AWDL as the standard NAN protocol, an iterative back-and-forth process with other Wi-Fi Alliance participants has resulted in the latest version of a standardised NAN protocol, now called Wi-Fi Aware. The standardised Wi-Fi Aware protocol now diverges from the proprietary AWDL protocol to the extent that they are incompatible with one another.

²³⁰ [...]

²³¹ [...]

²³² [...]

²³³ [...]

²³⁴ Apple’s reply to RFI 1 of 23 September 2024, question 15; Apple’s internal document, [...] page 20.

²³⁵ Technical meeting Apple/Commission of 3 October 2024, slide deck page 10; Apple’s reply to RFI 3, question 16.

²³⁶ Apple’s reply to RFI 3 of 7 October 2024, question 3.

(202) Apple's own services and hardware predominantly use AWDL to share data across AWDL-capable Apple devices (e.g. AirDrop) [...] ²³⁷ AWDL currently supports the rates and channels of Wi-Fi 2 (802.11a/g) through Wi-Fi 6E (802.11ac). ²³⁸ [...] ²³⁹

(203) [...] ²⁴⁰ [...] ²⁴¹

5.4.4. Current implementation for third-party services and hardware

(204) Apple provides third party iOS app developers with different options in order to establish a Wi-Fi connection between Apple devices or between an Apple and a third-party connected physical device. However, the Wi-Fi communication protocols available to third parties to establish a connection between Apple and third-party connected physical devices face a number of constraints.

(205) Third-party app developers can establish an AWDL connection between two Apple devices using two different frameworks, namely the *MultipeerConnectivity* and *Network* frameworks. ²⁴² Neither these frameworks nor any other frameworks allow third-party app developers to establish AWDL connections between an Apple and a third-party connected physical device, as AWDL is a proprietary protocol that Apple has not made available to third-party hardware providers. ²⁴³ There are no frameworks currently available to third parties to establish a Wi-Fi Aware connection.

(206) Third parties can establish a Wi-Fi connection (but not a P2P Wi-Fi connection) between an iOS device and a third-party connected physical device using three Wi-Fi connection types. Each of these options is inferior to a P2P Wi-Fi connection, including because they require either the use of a local infrastructure Wi-Fi or that one of the devices has a cellular internet connection.

(a) *First*, third-party app developers can use infrastructure Wi-Fi via the *Network* framework to transfer data between an Apple and a third-party connected physical device. ²⁴⁴ However, using infrastructure Wi-Fi implies that both devices involved in a data transfer are connected to infrastructure Wi-Fi. This means that the Wi-Fi connection is not independent of a local Wi-Fi connection.

(b) *Second*, third-party app developers can establish a Wi-Fi hotspot connection between an iOS device and a third-party connected physical device via the *NEHotspotConfiguration* APIs of the *Network Extension* framework. The APIs allow companion iOS apps to request an iPhone to join a Wi-Fi hotspot that is provided by a connected physical device that acts as an access point. ²⁴⁵ However, this connection through a hotspot (i) involves user prompts whenever a connection is supposed to be established between an Apple and a

²³⁷ Apple's reply to RFI 1 of 23 September 2024, question 15; Apple's internal document, [...], page 8.

²³⁸ Apple's reply to RFI 7 of 8 November 2024, question 3.

²³⁹ Apple's reply to RFI 3 of 7 October 2024, question 12.

²⁴⁰ Technical meeting Apple/Commission of 3 October 2024, slide deck page 10 and Apple's reply to RFI 3 of 7 October 2024, question 7; Apple's internal document, [...], page 14.

²⁴¹ Apple's reply to RFI 3 of 7 October 2024, question 7.

²⁴² Apple's reply to RFI 1 of 23 September 2024, question 23.

²⁴³ Apple's reply to RFI 1 of 23 September 2024, questions 19 and 23.

²⁴⁴ Apple's reply to RFI 1 of 23 September 2024, question 23.

²⁴⁵ [Third-party developer]'s reply to RFI 1 of [Confidential], questions 2 and 8 and [third-party developer]'s submission of 15 October 2024, Table 1.

third-party connected physical device, which means that (ii) a connection cannot be established automatically in the background, (iii) implies a high battery consumption of the third-party connected physical device on which the hotspot is launched, and (iv) prevents the iOS device from maintaining its connection with infrastructure Wi-Fi in parallel, meaning that the iOS device needs to revert back to a cellular connection if internet access is needed, provided that a cellular network is available.²⁴⁶

- (c) *Third*, a third-party app developer can establish a Wi-Fi hotspot connection between an iOS device and a third-party connected physical device by directing end users to use their iOS device as a hotspot which the third-party connected physical device can join.²⁴⁷ However, using an iOS hotspot (i) involves user prompts whenever a connection is supposed to be established between an Apple and a third-party connected physical device, (ii) cannot be established automatically in the background as user consent is required, (iii) implies a high battery consumption of the iPhone, and (iv) prevents the iOS device from maintaining its connection with infrastructure Wi-Fi in parallel, meaning that the iOS device needs to revert back to a cellular connection if internet access is needed, provided that a cellular network is available.
- (d) Therefore, the Commission considers that there is currently an interoperability gap when it comes to third-party connected physical devices connected to iOS devices and that it should specify how Apple has to fill this gap to effectively comply with Article 6(7) of Regulation (EU) 2022/1925.

5.4.5. *The gatekeeper's view*

- (207) In its response to the Preliminary Findings, Apple proposes to introduce Wi-Fi Aware [...] to provide effective interoperability with the P2P Wi-Fi connection feature on iOS for third-party connected physical devices.²⁴⁸

5.4.5.1. Concerning the AWDL interoperability solution

- (208) Apple submits that the Preliminary Findings err in assuming that AWDL could provide effective interoperability with the P2P Wi-Fi connection feature for third-party connected physical devices.²⁴⁹ [...]

5.4.5.2. Concerning the Wi-Fi Aware interoperability solution

- (209) Although Apple submits a Wi-Fi Aware proposal, Apple considers that the Preliminary Findings erroneously interpret “*feature*” to encompass granular details of Apple’s P2P Wi-Fi connection feature²⁵⁰ and that effective interoperability does not require interoperability with “*all functionalities*” of a feature.²⁵¹ The Preliminary Findings go beyond what is necessary to provide effective interoperability with the

²⁴⁶ [Third-party developer]’s reply to RFI 1 of 13 June 2024, question 16; [third-party developer]’s reply to RFI 1 of [...], questions 2, 7, and 8; [third-party developer]’s submission of 15 October 2024, Table 1; Apple’s internal document, [...], page 6.

²⁴⁷ [Third-party developer]’s submission of 15 October 2024, Table 1.

²⁴⁸ Apple’s reply to the Preliminary Findings, paragraphs 174 and 188.

²⁴⁹ Apple’s reply to the Preliminary Findings, paragraphs 175-187.

²⁵⁰ Apple’s reply to the Preliminary Findings, paragraphs 190-191 and footnote 126.

²⁵¹ Apple’s mark-up of the proposed measures of 23 January 2025, comment [A23].

P2P Wi-Fi connection feature²⁵² and even create additional tests that are unnecessary to ensure the continued effectiveness of Apple’s interoperability solution.²⁵³

- (210) *First*, Apple submits that the requirement to provide third parties with simultaneous access to any new functionalities in the Wi-Fi Aware implementation available to Apple goes beyond what is required for effective interoperability under Article 6(7) of Regulation (EU) 2022/1925.²⁵⁴ Not all differences between the iOS Wi-Fi Aware implementations available to Apple and third parties would render Apple’s interoperability solution ineffective and requiring simultaneous access prevents Apple from testing new implementation details internally.
- (211) *Second*, Apple submits that Article 6(7) of Regulation (EU) 2022/1925 provides no legal bases to require Apple to engage with third parties to improve the Wi-Fi Aware standards irrespective of whether the future functionalities are available to Apple’s services or hardware.²⁵⁵ In any event, the changes to the Wi-Fi Aware standard are subject to the assessment of Wi-Fi Alliance members and Apple’s proposals would not automatically become part of that standard.
- (212) *Third*, Apple submits that requiring Apple to support the newest Wi-Fi Aware standard after its adoption by the Wi-Fi Alliance within a reasonable timeframe is beyond the scope of Article 6(7) of Regulation (EU) 2022/1925.²⁵⁶ In particular, Apple argues that the measure cannot be imposed irrespective of (i) whether Apple’s own services and hardware have access to the additional functionality or (ii) whether Wi-Fi Aware develops into a less secure, privacy-preserving, or performant standard, which Apple would be compelled to support.
- (213) *Fourth*, Apple submits that requiring Apple to implement changes to AWDL in Apple’s adoption of Wi-Fi Aware at the same time and irrespective of whether they have become part of the Wi-Fi Aware standard is not feasible and not required for effective interoperability under Article 6(7) of Regulation (EU) 2022/1925 and may, in certain situations, not be technically feasible.²⁵⁷
- (214) *Fifth*, Apple submits that Article 6(7) of Regulation (EU) 2022/1925 does not include an obligation not to prevent technologies from becoming part of Wi-Fi Aware.²⁵⁸ Apple does not control the development of the standard in the Wi-Fi Alliance and cannot unilaterally block the inclusion of what might be considered to be an AWDL functionality in Wi-Fi Aware. In a later submission, Apple added that the measure imposes requirements “*irrespective of Apple’s IP.*”²⁵⁹

²⁵² Apple’s reply to the Preliminary Findings, paragraphs 190-191.

²⁵³ Apple’s reply to the Preliminary Findings, paragraph 191. Apple explains that the additional tests include whether Apple has (i) adopted the newest Wi-Fi Aware standard, (ii) provided third-party developers with access to new Wi-Fi Aware functionalities at the same time as to its own, or (iii) implemented new features of or updated its AWDL implementation also in its Wi-Fi Aware implementation.

²⁵⁴ Apple’s reply to the Preliminary Findings, paragraph 202; Apple’s mark-up of the proposed measures of 23 January 2025, comments [A27] and [A28].

²⁵⁵ Apple’s reply to the Preliminary Findings, paragraphs 192-195.

²⁵⁶ Apple’s reply to the Preliminary Findings, paragraph 196; Apple’s mark-up of the proposed measures of 23 January 2025, comment [A30].

²⁵⁷ Apple’s reply to the Preliminary Findings, paragraphs 197-199.

²⁵⁸ Apple’s reply to the Preliminary Findings, paragraphs 200-201.

²⁵⁹ Email from Apple to the Commission on 13 February 2025 [on the draft final measures].

- (215) *Sixth*, Apple submits that requiring Apple to ensure that Wi-Fi chips of iOS devices have sufficient memory available to run two concurrent P2P Wi-Fi connections,²⁶⁰ which could require Apple, or its chipset vendors, to build a new technology rather than providing interoperability with an existing feature, goes beyond the scope of Article 6(7) of Regulation (EU) 2022/1925.²⁶¹
- (216) *Seventh*, Apple submits that the Preliminary Findings include a feature that is not available to Apple, namely establishing a Wi-Fi Aware connection that serves as a hotspot providing internet access to a connected physical device using the concurrent infrastructure Wi-Fi.²⁶²

5.4.5.3. Concerning timing

- (217) Apple first submits that it is not technically feasible for Apple to develop the Wi-Fi Aware interoperability solution by fall 2025, as the specification of the Wi-Fi 5.0 standard, which includes a number of required technologies for Apple's interoperability solution, is only expected to be available by early 2026.²⁶³ [...] ²⁶⁴ [...] ²⁶⁵ [...]

5.4.6. *The Commission's assessment*

- (218) As set out in the Preliminary Findings, the Commission considers that the implementation of either an AWDL or Wi-Fi Aware solution could constitute effective ways to provide interoperability with the P2P Wi-Fi connection feature under Article 6(7) of Regulation (EU) 2022/1925.²⁶⁶ Apple proposes to provide interoperability with the P2P Wi-Fi connection feature through Wi-Fi Aware, as it considers AWDL not to be suitable for interoperability.²⁶⁷ Without prejudice as to whether the Commission considers AWDL to be within the scope of Article 6(7) of Regulation (EU) 2022/1925, the Commission considers that Apple's proposed Wi-Fi Aware interoperability solution could provide effective interoperability with the P2P Wi-Fi connection feature.
- (219) Regarding the two alternative interoperability solutions for the P2P Wi-Fi connection feature, Apple had proposed Wi-Fi Aware [...] ²⁶⁸ [...] The Commission considers that it could constitute a material change of the facts onto which this Decision is based, should Apple not deprecate AWDL in due time, and/or were a functionality gap to exist between Apple's AWDL implementation and the iOS Wi-Fi Aware implementation available to third parties. If this change of facts would materialise, the Commission considers that effective compliance with Article 6(7) of Regulation (EU) 2022/1925 may require Apple to make AWDL interoperable, as Apple must provide third parties with an equally effective P2P Wi-Fi connection feature as is

²⁶⁰ Running two concurrent P2P Wi-Fi connections implies that iOS devices can support both, AWDL or Wi-Fi Aware connections, and not just the P2P Wi-Fi solution that is only available to Apple (i.e. AWDL).

²⁶¹ Apple's reply to the Preliminary Findings, paragraph 203.

²⁶² Apple's reply to the Preliminary Findings, footnote 151.

²⁶³ Apple's reply to the Preliminary Findings, paragraphs 204-205 and 220.

²⁶⁴ Email from Apple to the Commission of 3 February 2025 [...].

²⁶⁵ Email from Apple to the Commission on 17 February 2025 [on the draft final measures].

²⁶⁶ Preliminary Findings, paragraph 119.

²⁶⁷ Apple's reply to the Preliminary Findings, paragraphs 174 and 188. According to Apple, the alternative interoperability solution proposed by the Commission in the Preliminary Findings, namely AWDL, cannot be required under Article 6(7) of Regulation (EU) 2022/1925.

²⁶⁸ Technical meeting Apple/Commission of 3 October 2024, slide deck page 10.

available to Apple, regardless of whether the P2P Wi-Fi connection feature that is made available to third parties is based on AWDL or Wi-Fi Aware.

- (220) The Commission disagrees with Apple’s claim that a number of measures set out in the Preliminary Findings are not necessary for providing effective interoperability with Apple’s interoperability solution. As explained in Section 3.1.1 of this Decision, the Commission considers that Article 6(7) of Regulation (EU) 2022/1925 does not require the Commission to demonstrate that each of the measures is individually necessary to enable contestability, i.e. that (some) third parties are able to provide a “*competitive offering*” or an “*alternative solution*,” which is enough for achieving contestability. Such assessment would reintroduce the requirement to investigate on a case-by-case basis the effects on competition of a gatekeeper’s given conduct, which the legislator explicitly rejected and which is contrary to the text and purpose of Article 6(7) of Regulation (EU) 2022/1925. In particular, the measures set out in the Preliminary Findings ensure that third parties can interoperate with the same feature available to Apple in an equally effective way, including performance and user experience. For instance, there is no reason why Apple should be able to make future updates, including new functionalities, of its iOS Wi-Fi Aware solution available to third parties later than to itself, and thereby put third parties at a disadvantage – especially as Apple plans to use the public Wi-Fi Aware API.

5.4.6.1. Concerning developments to Apple’s iOS Wi-Fi Aware implementation

- (221) Regarding the measures foreseen in the Preliminary Findings concerned with the future developments of Apple’s iOS Wi-Fi Aware implementation (which may diverge from the Wi-Fi Aware standard), the Commission considers that, contrary to Apple’s claims²⁶⁹ and as set out in Section 3.1.3 of this Decision, once new features and functionalities become available to Apple’s services or hardware, Apple must make the feature available to third parties. As detailed in Section 3.1.3 of this Decision, this does not reduce Apple’s incentives to innovate or deprive Apple of its competitive advantage.
- (222) The Commission considers that the measure aims to ensure that Apple does not undermine effective interoperability by continuing to develop its P2P Wi-Fi connection feature (irrespective of whether through the AWDL or Wi-Fi Aware implementation) that Apple reserves for its own services and hardware, while ceasing support for the Wi-Fi Aware implementation it makes available to third parties. [...] ²⁷⁰ The measure aims to ensure that such a future functionality would be made available to third parties at the same time and under equal conditions as they become available to Apple’s services or hardware.

5.4.6.2. Concerning developments to the Wi-Fi Aware standard

- (223) Regarding the measures foreseen in the Preliminary Findings concerned with the future developments of the Wi-Fi Aware standard,²⁷¹ the Commission notes that the measures are explicitly limited to the functionalities available to Apple’s own services or hardware.

²⁶⁹ Apple’s reply to the Preliminary Findings, paragraph 202; Apple’s mark-up of the proposed measures of 23 January 2025, comments [A27] and [A28].

²⁷⁰ Apple’s submission of 7 November 2024, paragraph 14.

²⁷¹ Namely requiring Apple to (i) engage with third parties to improve the Wi-Fi Aware standard and (ii) update the iOS Wi-Fi Aware implementation to support the newest Wi-Fi Aware standard after its adoption by the Wi-Fi Alliance within a reasonable timeframe.

- (224) It is incorrect that the measures include an open-ended mandate to improve an industry standard irrespective of the developments of the standard or the long-term developments of Apple's technologies. Apple's obligations in that respect are limited to features available to Apple under the P2P Wi-Fi feature available to Apple, irrespective of whether the feature is available via the AWDL or Wi-Fi Aware implementation. The Commission considers that these obligations are necessary for effective compliance and proportionate; they are in fact the direct consequence of Apple's proposal to implement Wi-Fi Aware and consistent with its representation that it would deprecate AWDL in favour of Wi-Fi Aware in the long-run, see recital (219) of this Decision. It is true, and not contradicted by the measures, that the Wi-Fi Aware standard is subject to the assessment of Wi-Fi Alliance members and that Apple's proposal would not automatically become part of that standard.
- (225) In particular regarding the measure requiring Apple to engage with third parties to improve the Wi-Fi Aware standard, the Commission would like to point out that Apple had initially proposed the Wi-Fi Aware-based interoperability solution (see recital (219) of this Decision), which is based on the Wi-Fi Alliance standard. The Wi-Fi Alliance standard is developed within the Wi-Fi Alliance, of which Apple is a member. As P2P Wi-Fi is an evolving technology, standardisation effects regarding P2P Wi-Fi will continue. The Commission considers that Apple would act in bad faith, and in contradiction to its own proposal and declaration that it would deprecate AWDL in favour of Wi-Fi Aware, if it were to discontinue to constructively engage to or otherwise obstruct the work to improve the Wi-Fi Aware standard within the Wi-Fi Alliance. Such conduct would infringe the principle of *venire contra factum proprium*.
- (226) As regards Apple's claim that it cannot be required to update the iOS Wi-Fi Aware implementation to support the newest Wi-Fi Aware standard after its adoption by the Wi-Fi Alliance within a reasonable timeframe, the Commission points out that this measure in the Annex to this Decision is limited to functionalities that are available to Apple's services or hardware. Contrary to Apple's claims and as set out in Sections 3.1.3 and 5.4.6.1 of this Decision, once new features and functionalities become available to Apple's services or hardware, Apple must make the feature available to third parties.
- (227) As regards Apple's claim that Wi-Fi Aware standard may evolve to be less secure, less privacy preserving, and less performant than Apple's existing Wi-Fi Aware implementation, the Commission notes that this possibility is inherent in an interoperability solution based on a standard. Apple was well aware of this possibility when it proposed such a Wi-Fi Aware-based solution and, when proposing the solution, Apple did not raise such concerns. [...] ²⁷² [...] ²⁷³
- (228) The Commission further notes the requirements of the integrity justification set out in Section 3.3 of this Decision and that both, gatekeepers and third parties, are subject to legal requirements regarding security and privacy as set out in recital (679) of this Decision. Moreover, they are speculative at this stage.

²⁷² Apple's reply to RFI 3 of 7 October 2024, questions 4.

²⁷³ Apple's reply to the Preliminary Findings, paragraphs 180-184; Apple's reply to RFI 3 of 7 October 2024, questions 4 and 5.

5.4.6.3. Concerning developments to AWDL

- (229) Contrary to Apple's views regarding the measures concerned with the future developments of AWDL,²⁷⁴ the Commission notes that these obligations are necessary and proportionate. In particular, the measures aim to ensure that Apple does not undermine effective interoperability by continuing to develop the AWDL implementation it reserves for its own services or hardware while ceasing support for the Wi-Fi Aware implementation it makes available to third parties. [...]²⁷⁵
- (230) Regarding the measure requiring Apple to implement changes to AWDL in the iOS Wi-Fi Aware implementation available to third parties at the same time as they are available to Apple, the measure only applies if it possible to implement the AWDL functionality into the P2P Wi-Fi Aware implementation. Apple's concern that there may be situations in which Apple cannot technically implement a new AWDL functionality simultaneously into its Wi-Fi Aware implementation is therefore unfounded.
- (231) Regarding the measure requiring Apple not to prevent AWDL functionalities from becoming part of the Wi-Fi Aware industry standard, the Commission considers that if Apple were allowed to prevent AWDL functionalities from becoming part of the Wi-Fi Aware industry standard, then equal effectiveness would be undermined. As to Apple's argument that it cannot be compelled to support future versions of Wi-Fi Aware if third parties seek to make the Wi-Fi Aware standard less secure, less privacy preserving, or less performant, see recital (227) of this Decision. Furthermore, as regards Apple's argument that the Wi-Fi Aware standard is subject to the assessment of Wi-Fi Alliance members, meaning that, in practice, Apple could not prevent an AWDL-based functionality to become part of the Wi-Fi Aware standard, the Commission considers the claim to not contradict the measure.
- (232) At a very late stage of the proceedings Apple suggested in an email that the clause should be removed [because of IP concerns]²⁷⁶ Apple had not previously raised this point, particularly when it [proposed] Wi-Fi Aware [as a] P2P Wi-Fi interoperability solution. The Commission notes that Apple has not properly explained what its concern would be in this regard, taking into account the considerations in Section 6.1 of this Decision. In any case, Apple is permitted to submit a reasoned request pursuant to paragraph (102) of the Annex to this Decision and as laid out in Section 5.12.9 of this Decision. Apple may submit such request should it consider that compliance with this obligation is liable to violate Apple's right to property under Article 17 of the Charter. Apple should submit such request without undue delay.

5.4.6.4. Concerning the allocation of Wi-Fi chip memory for P2P Wi-Fi connections

- (233) Regarding Apple's claim that the proposed obligation to ensure that Wi-Fi chips of iOS devices have sufficient memory available to run two concurrent P2P Wi-Fi connections, goes beyond the scope of Article 6(7) of Regulation (EU) 2022/1925, the Commission notes that it clarified the measure to read that memory allocation for two concurrent P2P Wi-Fi connections should be done in a non-discriminatory way,

²⁷⁴ Namely, requiring Apple to (i) implement changes to AWDL in the iOS Wi-Fi Aware implementation available to third parties at the same time as they are available to Apple and (ii) not prevent AWDL functionalities from becoming part of the Wi-Fi Aware industry standard.

²⁷⁵ Technical meeting Apple/Commission of 3 October 2024, slide deck page 10; Apple's reply to RFI 3 of 7 October 2024, question 7; Apple's internal document, [...], page 14.

²⁷⁶ Email from Apple to the Commission on 13 February 2025 [on the draft final measures].

to ensure that third parties have access to the P2P Wi-Fi connection feature under equal conditions compared to Apple.

5.4.6.5. Concerning P2P Wi-Fi hotspots using a concurrent connection

- (234) Apple submits that establishing a P2P Wi-Fi connection that serves as a hotspot providing internet access to a connected physical device using the concurrent infrastructure Wi-Fi is currently not available to Apple's services or hardware. Such P2P Wi-Fi hotspotting is only available to Apple through a concurrent cellular connection. Furthermore, [third-party developer] suggested during the public consultation to make the measure conditional on whether the functionality is available to Apple. The Commission notes that the measure has been amended to take the feedback from Apple and the public consultation into account.

5.4.6.6. Concerning timing

- (235) Apple has had a significant amount of time to consider and work on an interoperability solution for the P2P Wi-Fi connection. Apple received the first formal requests for interoperability with a high-bandwidth P2P Wi-Fi connection in March 2024. At the same time, Apple has used most of the functionalities of its AWDL implementation of the P2P Wi-Fi connection feature for several years, meaning that these functionalities are likely well established and known.
- (236) [...]

5.4.7. *Measures that Apple should implement*

- (237) To meet the requirements of Article 6(7) of Regulation (EU) 2022/1925, Apple should implement an interoperability solution that provides third parties with access to the same high-bandwidth P2P Wi-Fi feature as available to Apple (described in Section 5.4.1 of this Decision), in a way that is equally effective as the solution available to Apple. For the avoidance of doubt, this includes using the P2P Wi-Fi connection feature between an iOS device and a nearby Apple or third-party connected physical device.
- (238) Apple should provide interoperability with all functionalities of the high-bandwidth P2P Wi-Fi connection feature which are available to Apple's own connected physical devices, including, but not limited to, Apple Vision Pro, Apple Watch, as well as any future Apple connected physical devices. The functionalities of the P2P Wi-Fi connection feature are listed in recital (196) of this Decision.
- (239) Apple should grant third parties access to additional functionalities to those referred to in the preceding recital if necessary to enable effective interoperability with the P2P Wi-Fi connection feature described in Section 5.4.1 of this Decision.
- (240) Apple should make Wi-Fi Aware available to third parties.²⁷⁷
- (241) Implementing a solution based on the use of Wi-Fi Aware means that Apple should allow third-party connected physical devices access to the same functionalities of the

²⁷⁷ The Commission also considered interoperability with Wi-Fi Direct (another standard for P2P Wi-Fi connections). However, there was no strong support for Wi-Fi Direct in response to the public consultation and the Commission understands Wi-Fi Aware to encompass the functionalities provided by Wi-Fi Direct, making Wi-Fi Aware the more versatile standard. See also [third-party developer]'s submission of 15 October 2024, paragraph 2.2; [Third-party developer]'s reply to RFI 1 of 4 October 2024, question 1.

P2P Wi-Fi connection feature as available to Apple's own connected physical devices. This means in practice that Apple should:

- (a) implement Wi-Fi Aware in its iOS devices and iOS in accordance with the Wi-Fi Aware specification unless Apple demonstrates that it is not necessary to ensure that third parties have access to the same functionalities and in an equally effective way as Apple's own connected physical devices under its own implementation of P2P Wi-Fi;
- (b) allow third parties to establish a Wi-Fi Aware connection between an iOS device and any third-party connected physical device that supports Wi-Fi Aware;
- (c) allow third parties to establish a Wi-Fi Aware connection on-demand, without further user intervention via the companion app or otherwise, or without more user intervention than is required between Apple devices to establish a P2P Wi-Fi connection;²⁷⁸
- (d) allow third parties to establish a Wi-Fi Aware P2P connection with an iOS device, while the iOS device can maintain an infrastructure Wi-Fi connection in parallel. Furthermore, Apple should implement a non-discriminatory channel switching policy that is most suitable for its own and third-party use cases;²⁷⁹
- (e) allow third parties access to the same connection metadata and to configure the same parameters of the Wi-Fi Aware connection as Apple uses itself in its P2P Wi-Fi connection solution;
- (f) to the extent technically possible, ensure that the Wi-Fi chip of iOS devices, including legacy devices, allocate the memory available to support two concurrent P2P Wi-Fi connections in a non-discriminatory way, until Apple deprecates AWDL;²⁸⁰
- (g) continue to constructively engage with Wi-Fi Alliance participants to further improve the Wi-Fi Aware standard regarding any functionality available to Apple's own connected physical devices under its own implementation of P2P Wi-Fi; in the absence of legitimate and substantiated IPR concerns, Apple should not prevent, explicitly or de facto, functionalities available under its own implementation of P2P Wi-Fi from becoming part of the Wi-Fi Aware standard;
- (h) update the iOS Wi-Fi Aware implementation to support the newest Wi-Fi Aware standard after its adoption by the Wi-Fi Alliance within a reasonable timeframe regarding any functionality available to Apple's own connected physical devices under its own implementation of P2P Wi-Fi, unless Apple demonstrates that effective interoperability with the same functionality already exists;²⁸¹ for the avoidance of doubt, this includes supporting the wireless

²⁷⁸ [Third-party developer]'s reply to RFI 1 of [Confidential], question 7.

²⁷⁹ Apple's reply to RFI 3 of 7 October 2024, Table 3.

²⁸⁰ In Apple's reply to RFI 6 of 23 October 2024, question 2 and footnotes 2-3, Apple states that the legacy iOS devices that could support Wi-Fi Aware (in addition to the existing AWDL) are, subject to further verifications by Apple, the devices including and following the iPhone 11 series.

²⁸¹ Apple's submission of 7 November 2024, paragraph 25 and Table 1.

communication standards that are available to Apple's own connected physical devices.²⁸²

- (242) To the extent technically possible, Apple should provide third parties with a Wi-Fi Aware implementation in a way that is equally effective as its own implementation of P2P Wi-Fi. Until AWDL is deprecated, Apple must ensure, to the extent technically possible, that the solution made available to third parties is equally effective to the solution made available to Apple's connected physical devices, including in terms of set-up speed, bandwidth, transfer speed, performance, latency and uptime.²⁸³
- (243) Apple should also provide effective interoperability with any future updates, including new functionalities, of the P2P Wi-Fi connection feature, including with future functionalities of AWDL, insofar they are available to Apple's own connected physical devices. To this end, the general measures in Section 5.12 of this Decision apply, including in particular the measures concerning future updates and new functionalities set out in Section 5.12.7 in this Decision. This applies regardless of whether the future functionalities are part of the Wi-Fi Aware standard, unless Apple demonstrates that it is not possible to incorporate them into the P2P Wi-Fi implementation based on Wi-Fi Aware. In addition, in the absence of legitimate and substantiated IPR concerns, Apple should not prevent, explicitly or de facto, future updates, including new functionalities, of AWDL from becoming part of the Wi-Fi Aware standard. The future functionalities of the P2P Wi-Fi connection feature of which the Commission is aware of are listed in recital (197) of this Decision.
- (244) Apple should implement the measures above in compliance with the measures for all features in Section 5.12 of this Decision.

5.4.8. *Implementation timing*

- (245) Apple should provide effective interoperability with the P2P Wi-Fi connection feature by implementing the measures for Wi-Fi Aware 4.0 in the next major iOS release, i.e. iOS 19, at the latest, and for Wi-Fi Aware 5.0 in the next iOS release at the latest nine months following the introduction of the Wi-Fi Aware 5.0 specification.

5.5. **Measures for proximity-triggered pairing**

- (246) An iPhone user can pair a new set of AirPods (Apple's wireless earbuds), with their iPhone easily and quickly: they just need to bring the AirPods close to the iPhone. The iPhone will then automatically display a pop-up to the user that will start the pairing process. This proximity-triggered pairing process is easy, quick, and user-friendly, which is why it is referred to as "*magic pairing*". There is no need for the user to install first manually install any app: proximity-triggered pairing is supported out-of-the-box on iOS. Apple's connected physical devices – including AirPods, AirTags, and the Apple Watch – can use this proximity-triggered feature thanks to interoperability with iOS that Apple reserves to its own connected physical devices.

²⁸² Apple's reply to RFI 7 of 8 November 2024, question 3.

²⁸³ If Apple were to continue using AWDL, it could further develop AWDL while the development of Wi-Fi Aware is pursued in the framework of the Wi-Fi Alliance. A possible result could be that the Wi-Fi Aware implementation available to third parties may become inferior to the AWDL implementation used by Apple's own services. This would give rise to an interoperability gap, as P2P Wi-Fi connections between Apple devices via AWDL would be superior to those between an Apple device and a third-party connected physical device via Wi-Fi Aware.

- (247) Third-party connected physical devices do not enjoy the same level of interoperability with iOS. For example, users who want to pair third-party wireless headphones must find and pair them manually in the Bluetooth section of iOS settings, or must manually install the headphone’s companion app (if such an app exists) and then initiate the pairing process within it. This contrasts with other mobile operating systems, which support out-of-the-box proximity-triggered pairing for third-party connected physical devices.
- (248) Developers have requested interoperability with the proximity-triggered pairing feature for a long time before the submission of requests for the feature pursuant to Article 6(7) of Regulation (EU) 2022/1925. According to one developer, the wider developer community has been asking for interoperability with this feature since 2014.²⁸⁴

5.5.1. *Description of the feature*

- (249) The proximity-triggered pairing feature consists in the ability of third-party connected physical devices to pair and set up with an iOS device through the same proximity-triggered procedure that Apple uses for its own connected physical devices.
- (250) To use a connected physical device with an iOS device, that device must be “paired with” the iOS device. Apple connected physical devices can be paired with an iOS device for the first time through a proximity-triggered procedure. Proximity-triggered pairing works out-of-the-box: there is no need for the user to install any app beforehand and the feature automatically works for any connected physical device for which Apple has implemented support.
- (251) To enable this proximity-triggered pairing, the Apple connected physical device advertises the required device information via BLE while the iPhone is in a constant “listening” or “receiving” mode.²⁸⁵ [...] ²⁸⁶ [...] ²⁸⁷
- (252) If the Apple connected physical device, in this case the Apple Watch, is not yet paired to a different Apple iOS device, the iOS device will automatically display a pop-up prompting the user to initiate pairing and connect the Apple Watch with the iPhone (see Figure 6 below).

²⁸⁴ Technical meeting [third-party developer]/Commission of 2 May 2024, slide deck page 13.

²⁸⁵ Apple’s reply to RFI 3 of 7 October 2024, questions 37 to 43.

²⁸⁶ Apple’s reply to RFI 3 of 7 October 2024, questions 37 to 43.

²⁸⁷ Apple’s reply to RFI 3 of 7 October 2024, question 43.

Figure 6: Proximity-triggered pairing between an iOS device and an Apple Watch



Source: <https://support.apple.com/en-us/109015>, accessed on 6 November 2024.

- (253) If the end user selects to continue with the pairing process, they need to complete a further verification step (as shown in Figure 7 below). The user is then automatically prompted to the set-up menu of the Apple Watch app, the companion app of the Apple Watch, which is pre-installed on every iOS device.²⁸⁸

Figure 7: Confirmation of pairing between an iOS device and an Apple Watch



Source: <https://support.apple.com/en-us/109015>, accessed on 6 November 2024.

- (254) A similar user experience is supported for Apple's AirPods – a set of wireless Bluetooth earbuds. As soon as the user brings the AirPods in the proximity of the

²⁸⁸ Apple's reply to RFI 3 of 7 October 2024, question 36.

iOS device, these are automatically discovered, and a pop-up is shown to the user (see Figure 8).²⁸⁹

Figure 8: Proximity-triggered pairing between an iOS device and AirPods Pro



Source: Technical meeting Apple/Commission of 3 October 2024, slide deck page 25.

- (255) Proximity-triggered pairing is used for the initial set-up of the connected physical device. Once paired, a connected physical device can be used and automatically reconnected to the iOS device. Subsequent pairing is only necessary if the connected physical device is removed by the end user from the list of paired devices in iOS settings.

5.5.2. *Feature falls within the scope of Article 6(7) of Regulation (EU) 2022/1925*

- (256) The Commission finds that the proximity-triggered pairing feature as described in Section 5.5.1 of this Decision – together with its functionalities – falls within the scope of Article 6(7) of Regulation (EU) 2022/1925. Proximity-triggered pairing is a hardware and software feature which is controlled via iOS, Apple’s operating systems for iPhones, which is listed in the Designation Decision.

5.5.3. *Current implementation for Apple’s own services and hardware*

- (257) Proximity-triggered pairing is available to and used by Apple, for example for its Apple Watch. Apple specifically markets the ease and speed of the pairing and set-up process of the Apple Watch: “It takes just a few minutes to get up and running with Apple Watch.”²⁹⁰ The proximity-triggered pairing feature allows Apple to limit the instructions for the pairing of the Apple Watch to one simple sentence: “Bring your iPhone near your [Apple] Watch, then follow the onscreen instructions.”²⁹¹

²⁸⁹ Due to the lack of a dedicated AirPods companion app and of a screen on the AirPods, there is no further verification step.

²⁹⁰ See <https://support.apple.com/guide/watch/get-started-with-apple-watch-apd1456230aa/watchos>, accessed on 6 November 2024.

²⁹¹ See <https://support.apple.com/guide/watch/get-started-with-apple-watch-apd1456230aa/watchos>, accessed on 6 November 2024.

- (258) [...] ²⁹² According to the information available to the Commission, iOS continuously scans for BLE advertisements from the Apple Watch that the watch wants to initiate setup. ²⁹³ The automatic pairing of an Apple Watch with an iPhone then occurs when the iPhone receives such a BLE advertisement while the user holds the iPhone near the Apple Watch [...]. ²⁹⁴ iOS surfaces the Apple Watch pairing screen to appear on the iPhone, and the user then taps Continue. ²⁹⁵
- (259) Consequently, to use proximity-triggered pairing between an iOS device and an Apple connected physical device, the end user does not need to manually enable the function or activate a dedicated pairing mode, nor having to interact with iOS settings. Furthermore, the end user does not have to download, install, or open any app on the iPhone to use proximity-triggered pairing. [...] The entire pairing process is carried out within the pop-up prompts displayed by the iPhone.
- (260) As regards Apple's AirPods, there is no need for the user to install software specifically to be able to pair them "magically" with the iPhone. Apple has explained that this software is integrated into iOS. ²⁹⁶
- 5.5.4. *Current implementation for third-party services and hardware*
- (261) It is currently not possible for third-party manufacturers to use the "magic" device discovery experience unless Apple provides interoperability with the proximity-triggered pairing feature.
- (262) To the Commission's knowledge, ²⁹⁷ third-party connected physical devices that support the BLE protocol can be paired with an iOS device via the *Core Bluetooth* framework. However, in contrast to the proximity-triggered pairing feature available to Apple's connected physical devices, the pairing of third-party connected physical devices cannot be initiated via out-of-the-box proximity-triggered device discovery. Furthermore, the pairing process for certain third-party connected physical devices requires the identification and download of the companion app before the pairing process. For example, the pairing of third-party connected smartwatches with an iOS device via the *Core Bluetooth* framework requires the steps listed below.
- (a) *First*, the end user needs to identify and download the appropriate companion app for the respective connected physical device.
 - (b) *Second*, once the user has opened the companion app, they need to give explicit permission for the companion app to access Bluetooth on the iOS device.
 - (c) *Third*, the end user needs to initiate the Bluetooth pairing process in the companion app.
 - (d) *Fourth*, once the third-party connected physical device has been discovered via Bluetooth, the end user needs to confirm the pairing. ²⁹⁸
- (263) In iOS 18, Apple introduced *AccessorySetupKit*, a framework for the discovery and configuration of Bluetooth or Wi-Fi connected physical devices. ²⁹⁹

²⁹² Apple's reply to RFI 2 of 30 September 2024, Annex 1.2.

²⁹³ [...]

²⁹⁴ Apple's reply to RFI 3 of 7 October 2024, question 3.

²⁹⁵ Apple's reply to RFI 2 of 30 September 2024, Annex 1.2.

²⁹⁶ Apple's reply to RFI 3 of 7 October 2024, question 41.

²⁹⁷ Apple's reply to RFI 2 of 30 September 2024, Annex 1.2.

²⁹⁸ See for instance [third-party developer]'s reply to RFI 1 of 18 June, question 10, attachment [...].

AccessorySetupKit enables third-party developers to present a system user interface through their companion apps that enables users to initiate discovery of a specific type of device. Once a user has decided to find and pair a device, *AccessorySetupKit* allows the user to complete those actions through a single user interface, provided by Apple, that Apple considers to be comparable with the user interface used for Apple's own connected physical devices.

- (264) However, *AccessorySetupKit* does not offer the same functionalities as proximity-triggered pairing. It does not enable out-of-the-box proximity-triggered discovery and pairing of third-party connected physical devices. Using *AccessorySetupKit*, end users need to download the companion app for a device to be able to be discovered and paired with the iPhone.
- (265) Therefore, despite having solutions for third parties to pair their devices with the iPhone, end users cannot pair their third-party connected physical devices as seamlessly and using this streamlined simplified pairing procedure with the iPhone as end users of Apple connected physical devices.
- (266) Therefore, the Commission considers that there is currently an interoperability gap when it comes to third-party connected physical devices connected to iOS devices and that it should specify how Apple has to fill this gap to comply with Article 6(7) of Regulation (EU) 2022/1925.

5.5.5. *The gatekeeper's view*

- (267) Apple argues that Article 6(7) of Regulation (EU) 2022/1925 does not mandate interoperability with the proximity-triggered pairing feature. Apple considers that its current pairing solution, *AccessorySetupKit*, already provides for effective interoperability.³⁰⁰ Furthermore, Apple submits that the Commission failed to assess the feedback from developers,³⁰¹ and it considers that the Preliminary Findings go beyond what is required by Article 6(7) of Regulation (EU) 2022/1925 to provide for effective interoperability, including mandating continuous pairing, parity of pairing flows and the automatic download of a companion app.³⁰²
- (268) Apple contests the qualification of proximity-triggered pairing as a hardware or software feature. Apple defines the feature as a “*technology designed to establish a more convenient connection between Bluetooth devices and the iPhone,*” therefore it is not a requirement or a prerequisite for devices to connect to an iPhone via Bluetooth.³⁰³
- (269) Apple claims that enabling of out of-the-box proximity-triggered discovery and pairing of third-party connected physical devices as well as the ability for a device to

²⁹⁹ Technical meeting Apple/Commission of 3 October 2024, slide deck page 27; Apple's reply to RFI 3 of 7 October 2024, question 32.

³⁰⁰ Apple's reply to the Preliminary Findings, paragraph 300.

³⁰¹ According to Apple, the Commission did not consider the feedback of developers when assessing *AccessorySetupKit* and it challenges as well the importance of this feature for developers. See also Apple's reply to the Preliminary Findings, paragraphs 310-312 and 378, in which Apple claims that “*there is no evidence of developers requests of interoperability with this feature since 2014.*”

³⁰² Apple's reply to the Preliminary Findings, paragraphs 303 and 318-325; Preliminary Findings, paragraph 144.

³⁰³ Apple's reply to the Preliminary Findings, paragraphs 306-308.

be discovered and paired with the iPhone without the need of a prior download of the companion app are not required for effective interoperability.³⁰⁴

(270) [...] ³⁰⁵ [...] ³⁰⁶ [...] ³⁰⁷ [...] ³⁰⁸

(271) Apple considers the timeline which the Commission included in the Preliminary Findings for the implementation of the measures as “*unrealistic*.”

(272) Finally, on 17 February 2025, Apple sent further comments on the Draft Final Measures³⁰⁹ in which it explained for proximity-triggered pairing that [...] ³¹⁰

5.5.6. *The Commission’s assessment*

(273) The Commission observes the following regarding Apple’s submissions.

(274) *First*, the proximity-triggered pairing feature includes all the functionalities described in Section 5.5.1 of this Decision. As described in Section 3.1.2 of this Decision, whenever a feature consists of several functionalities, effective interoperability with that feature requires interoperability with all of those functionalities. Providing access to only some functionalities of a feature would not amount to full and effective interoperability with that same feature and would be contrary to the objective of Article 6(7) of Regulation (EU) 2022/1925 to create a level playing field. Under Apple’s very narrow definition of the respective feature, i.e. the feature being the mere ability to establish a connection between the iPhone proximity-triggered pairing, third parties would not have access to the same functionalities and features as available to Apple’s hardware and services, and thus they would not be able to offer services and hardware on an equal footing. Third parties consider proximity-triggered pairing important. There have been three requests for interoperability with this feature in 2024.³¹¹

(275) *Second*, as regards *AccessorySetupKit* as a possible interoperability solution, the Commission considers that it is not obliged in specification proceedings to assess whether this solution would effectively comply with Article 6(7) of Regulation (EU) 2022/1925 (see Section 2.3 of this Decision).

(276) Moreover, as pointed out in the Preliminary Findings,³¹² the Commission considered that this solution does not allow third-party connected physical devices to pair with the iPhone as seamlessly and simply as end users of Apple connected physical devices. For example, within *AccessorySetupKit*, end users must first download the companion app of the device outside the pairing process. A seamless end user flow

³⁰⁴ Apple’s reply to the Preliminary Findings, paragraph 313.

³⁰⁵ Apple’s submission of 7 November 2024; Apple’s reply to the Preliminary Findings, paragraphs 315-318.

³⁰⁶ In Apple’s mark-up of the Commission’s proposed measures of 23 January[...].

³⁰⁷ Apple’s reply to the Preliminary Findings, paragraph 316.

³⁰⁸ Apple’s reply to the Preliminary Findings, paragraph 318.

³⁰⁹ Email from Apple to the Commission on 17 February 2025 [on the draft final measures].

³¹⁰ Email from Apple to the Commission on 17 February 2025 [on the draft final measures]: [...].

³¹¹ One submitted by [third-party developer] on 19 January 2024 through Apple’s “Feedback Assistant” system, one submitted by [third-party developer] on 9 March 2024 through the Interoperability Request Portal and one submitted by [third-party developer] on 26 April through the Interoperability Request Portal.

³¹² Preliminary Findings, paragraphs 139-141.

without the need to first download the companion app is essential to the proximity-triggered pairing feature. [...] ³¹³

- (277) Developers also questioned *AccessorySetupKit* as an effective interoperability solution for various reasons, including the fact that it does not support automatic pairing and detection of third-party connected physical devices, and the fact that the prompts displayed to pair the device are “*alarming*”. ³¹⁴ [...] ³¹⁵
- (278) In addition to this, feedback received during the public consultation emphasized the relevance and need of having effective interoperability with this feature. ³¹⁶
- (279) *Third*, the Preliminary Findings set out the measures and functionalities which are required to ensure effective interoperability with this feature. Unlike Apple claims, having a continuous pairing flow or ensuring that Apple does not include more screens or user prompts compared to those it shows to users of its own connected physical devices, are functionalities and measures required to ensure effective interoperability with the proximity triggered feature.
- (280) *Fourth*, as regards the implementation timeline for the proximity-triggered pairing feature, the Commission considers that Apple should implement an interoperability solution as soon as possible. Apple has had a significant amount of time to consider and work on an interoperability solution for this feature. Apple has been aware of the lack of third parties’ ability to provide users with a streamlined user journey for the setup of third-party connected physical devices, at least since January 2024. ³¹⁷ At the same time, Apple has used this feature for its own products and services, thus the feature is well known to Apple. Nevertheless, having assessed Apple’s arguments regarding the technical complexity of the implementation of the new proposed solution, the fact that the certification process needs to be set up, and that additional engineering steps need to be undertaken to ensure that the interoperability solution works and is stable, the Commission considers that Apple’s timeline proposal is the most reasonable way going forward.
- (281) Finally, following the public consultation and the review of Apple’s submission and comments, the Commission has modified the initial proposed measures Apple is to implement. As explained in recital (270) of this Decision, Apple offered a new interoperability solution. The Commission has reflected this proposal as well as the

³¹³ See Apple’s internal document [...].

³¹⁴ [Third-party developer]’s reply to RFI 1 of [...], Question 8.e.iii.

³¹⁵ For instance, see Apple’s internal document, [...].

³¹⁶ [...] Importantly, in January, March and April 2024, three providers of connected physical devices requested interoperability with the seamless proximity-based pairing feature (see recital (121)(c) of this Decision). In addition to the general positive feedback received on the Proposed Measures during the public consultation, the proximity-pairing triggered measures were subject of support from several respondents. See for example the public consultation feedback from [third-party developer], explaining that “*These reports are exactly in line with what we were hoping to see*”; [association] stating that “[*association*] welcomes the measures that stipulate equivalence [...] the end user journey for proximity-triggered pairing should also be equivalent”; [third-party developer]; [third-party developer]: “*The measures proposed by the EC cover key features*”; [third-party developer]; [third-party developer] “*strongly supports the Commission’s Provisional Findings*” and specifically identifies the measures for the proximity-triggered pairing feature as one of the proposals that would provide a better fair playing field; [third-party developer]; [third-party developer].

³¹⁷ See the interoperability request submitted by [third-party developer] on 19 January 2024 through Apple’s “Feedback Assistant” system.

feedback of developers (including the need for a registration program),³¹⁸ Apple's mark-up of the Commission's proposed measures of 23 January 2025, and Apple's subsequent submissions and comments in the measures below.

5.5.7. *Measures that Apple should implement*

- (282) To meet the requirements of Article 6(7) of Regulation (EU) 2022/1925, Apple should implement an interoperability solution that provides third parties with access to the same proximity-triggered pairing feature as available to Apple (as described in Section 5.5.1 of this Decision), in a way that is equally effective as the solution available to Apple.
- (283) This means that third-party connected physical devices must have access to the same proximity-triggered pairing feature as available to Apple's own connected physical devices. Apple should provide interoperability with all functionalities of the proximity-triggered pairing feature that are available to Apple's own connected physical devices, including, but not limited to, AirPods, Apple Vision Pro, Apple Watch, as well as any future Apple connected physical devices. Each of these functionalities falls within the scope of Article 6(7) of Regulation (EU) 2022/1925 as explained in recital (126) of this Decision. These functionalities are:
- (a) the ability of a third-party connected physical device to establish a Bluetooth data connection with an iOS device for pairing purposes;
 - (b) the ability for the pairing process between the third-party connected physical devices and the iOS device to be triggered by the proximity of the connected physical device to the iOS device;
 - (c) the ability for the third-party connected physical device to be automatically discovered³¹⁹ by the iOS device via the BLE protocol for the initiation of the pairing process without the need for the end user to first download a third-party companion app;
 - (d) the ability to carry out the pairing and setup of the third-party connected physical device with the iOS device as a continuous and guided process starting with the proximity-triggered detection and, at the third party's option, continuing within the third-party companion app;
 - (e) the ability to make use of the same end user journey and ease of use for end users, as technically possible given the possible need to install a companion app, which includes:
 - (1) showing the same user prompts (in terms of, *inter alia*, number, content, format and design) as shown for Apple's most comparable connected physical device;
 - (2) showing the same information screens (in terms of, *inter alia*, number, content, format and design) as shown for Apple's most comparable

³¹⁸ [...] During the tripartite meetings with [third-party developer] (agreed minutes of meeting with [third-party developer] on 17 January 2025) and in [third-party developer]'s contribution to the public consultation [third-party developer] explained it understood the need for a registration process for reasons of [...], however it highlighted the importance of having a quick registration process.

³¹⁹ When a user brings, for example, the AirPods close to the iPhone, the iPhone will then automatically display a pop-up to the user that will start the pairing process.

connected physical device, in as much as this is possible considering the device capability;³²⁰

- (3) limiting the necessary time and user engagement to the same level as required for pairing Apple's most comparable connected physical device, including the number of prompts and information screens; in particular, where the end user is prompted to initiate the pairing process with a third-party connected physical device, the third-party companion app of the third-party connected physical device must be capable of being opened or downloaded, at the determination of the third-party developer, seamlessly without an additional user prompt unless Apple shows an equivalent prompt for its own connected physical devices;
 - (f) the settings regarding device pairing, including the location of the settings (e.g. in iOS settings or in an app) and the scope of settings.
- (284) Apple should grant third parties access to additional functionalities if necessary to enable effective interoperability with the proximity-triggered pairing feature described in Section 5.5.1 of this Decision.
- (285) To enable out-of-the-box proximity-triggered device discovery, Apple may integrate a mapping between third-party connected physical devices and the expected contents of their BLE advertisements, the relevant companion app(s), as well as other necessary metadata (including, but not limited to, transmission power or security keys) into iOS. To obtain the necessary metadata for this mapping, Apple may set up a program for third-party connected physical device manufacturers to register their connected physical devices for the purpose of making use of the proximity-triggered pairing feature.
- (286) Apple should ensure that such devices are registered and can use the proximity-triggered pairing feature within 15 days following the submission of the registration request. This registration process must be carried out in the shortest delay possible. However, unexpected circumstances may arise, which Apple should be able to take into account without unduly delaying the process.³²¹ Therefore, in the event of circumstances delaying the registration and testing, which are beyond Apple's control, Apple should ensure that the devices are registered and can use the proximity-triggered pairing feature within no more than four weeks following the submission of the registration request.
- (287) For the purpose of ensuring that effective interoperability continues in the future, third parties must also have access to any future updates, including new functionalities, of the proximity-triggered pairing feature insofar as they are available to Apple's own connected physical devices. For example, if Apple updates the feature to extend the range of discoverability, this update should be made available to third parties as well. To this end, the general measures in Section 5.12 of this

³²⁰ Apple explained during the meeting of 11 February 2025 that different connected physical devices may have different capabilities, and therefore not all information screens may be relevant. See agreed minutes of the meeting of 11 and 12 February 2025. See also Email from Apple to the Commission on 13 February 2025 [on the draft final measures].

³²¹ In an email from Apple to the Commission on 17 February 2025 [on the draft final measures] and during the meeting of 11 February 2025 Apple explained [...]. See email from Apple to the Commission on 17 February 2025 [on the draft final measures] and agreed minutes of the meeting with Apple of 11 and 12 February 2025.

Decision apply, including in particular the measures concerning future updates and new functionalities set out in Section 5.12.7 in this Decision.

5.5.8. *Implementation timing*

- (288) Apple should implement the measures for the proximity-triggered pairing feature in a beta version of iOS available to developers by the end of 2025 at the latest.
- (289) Apple must then implement the measures for the proximity-triggered pairing feature for end users by 1 June 2026 at the latest.

5.6. **Measures for background execution**

- (290) To work as intended, many iOS apps and services must stay active and running even when the user is not actively using them, or must at least be able to timely resume their activity when necessary. For example, a music player app must be able to play music while the user is using other apps. Similarly, an alarm app must be able to trigger an alarm at the right time, even if the iPhone has been locked and with the screen off for hours overnight. An iOS app's capability to do so depends on whether iOS grants it adequate interfaces and sufficient system resources, also referred to as "background execution."
- (291) In the context of connected physical devices, background execution plays a crucial role to ensure effective interoperability between the iOS device and the connected physical device. For example, a weather app running on a smartwatch must be able to retrieve the latest weather updates from the internet. However, smartwatches often do not connect directly to the internet, but instead rely on the iOS device to obtain weather data via an iOS app or can use the iPhone's internet connection to fetch the weather data directly. Similarly, a smart alarm app that relies on sleep tracking to wake up the user at the best moment must be able to send sleep tracking data from the smartwatch to the iPhone almost in real time. In the same way, a smart blood glucose monitor must be able to reliably connect to the smartphone to relay a dangerously low glucose reading and send a text message to emergency contacts via the iPhone.³²²
- (292) As such, it is important that the smartwatch has continuous and/or timely access to the iPhone, enabling apps and services running on the smartwatch to connect to and use iPhone services, and that those iPhone services are available and responsive to the smartwatch, i.e. running in the background.
- (293) Apple's services and hardware, notably the Apple Watch, enjoy privileged interoperability with iOS background execution capabilities. For example, the Apple Watch can communicate with the iPhone at any time. However, the same level of interoperability is not available to third-party connected physical devices, which may prevent them from working as expected and result in a poor user experience.

5.6.1. *Description of the feature*

- (294) The background execution feature consists in the ability of third-party connected physical devices to execute actions on and communicate with an iOS device in a timely manner, in the same way as Apple connected physical devices can.

³²² See, for example, <https://apps.apple.com/us/app/dario-health/id571322125>: "Simply connect the Dario meter to your smartphone, and upon recording a dangerously low glucose reading in one drop of blood, the Dario app will prepare a complete text message, including current blood glucose level and GPS location, to send to up to 4 emergency contacts," accessed 18 November 2024.

- (295) This ability depends on whether iOS provides adequate interfaces and allocates sufficient system resources to the app or service.³²³ System resources include, but are not limited to, access to hardware memory and CPU processing capacity. This ability is also referred to as iOS allocating “runtime” to an app.
- (296) The background execution feature is important for the effective use of iOS companion apps, iOS sister apps (as defined in recital (138) of this Decision), and iOS processes³²⁴ in order to provide data and updates from and to the connected physical device. For instance, a smartwatch user expects up-to-date news or weather content on the smartwatch when engaging with it. This depends on the background execution capabilities of an iOS companion app that provides such data to the connected physical device’s OS, of an iOS sister app that provides such data to its corresponding sister app on the smartwatch, and/or of iOS processes that are involved in establishing and maintaining the connection between the smartwatch and the iOS device.
- (297) Apple connected physical devices have access to background execution on iOS devices in situations when third-party connected physical devices do not.
- (298) [...] ³²⁵ Apple may rely on background execution capabilities when an end user makes a voice command via Apple’s AirPods, which is then processed on the iPhone (which may be in lock-screen mode in the end user’s pocket) to provide a response by Siri. [...] Third parties should have access to the same background execution capabilities for their voice assistants and other apps.
- (299) As explained below, Apple connected physical devices enjoy privileged access to background execution (referred to as “Apple-only iOS background execution”) because of certain iOS processes that provide background execution capabilities to Apple connected physical devices, but not to third-party connected physical devices.
- (300) By contrast, third-party connected physical devices are allocated runtime by different iOS mechanisms and policies (referred to as “regular iOS background execution”), which are explained below. These rules allocate background execution capabilities to iOS apps, including companion and sister apps that offer functionalities to the third-party connected physical device.
- (301) [...] ³²⁶ [...] ³²⁷ [...] ³²⁸ [...] ³²⁹
- (302) The following functionalities of the background execution feature are available to Apple.
- (a) Background execution capabilities for iOS apps/processes. Access to the same background execution capabilities which Apple allocates to iOS apps and iOS processes with respect to Apple devices.

³²³ Apple’s reply to RFI 4 of 14 October 2024, question 16.

³²⁴ Relevant iOS processes enable functionality of iOS or the iOS device with respect to the connected physical device, e.g. regarding Bluetooth connectivity.

[...]

³²⁵ Apple’s reply to RFI 4 of 14 October 2024, question 17.

³²⁶ Apple’s reply to RFI 6 of 23 October 2024, question 20.

³²⁷ Apple’s reply to RFI 6 of 23 October 2024, question 20.

³²⁸ Apple’s reply to RFI 6 of 23 October 2024, question 20.

³²⁹ This refers to the situation where related apps from the same app developer are installed both on the iOS device and a connected physical device and expected to interact with each other. One example is a fitness app intended to exchange and synchronize (fitness) data among both apps.

- (b) Impact of user actions and choice. Access to the same background execution capabilities entails, in particular, being exposed and subject to the same limitations of these capabilities as a result of a user action. This includes the effect of an end user terminating an iOS companion app or sister app in the app switching menu (“force-quitting” or “force-killing”) or toggling the Wi-Fi or Bluetooth buttons in Control Centre. Further, it includes the presentation and effect of any prompt that allows the end user to make choices on the level of background execution to a connected physical device,³³⁰ including regarding time, place, and cadence.
- (c) Effective use. Access to functionalities that allow Apple to make effective use of its background execution capabilities, regardless of whether an active end user interaction took place (e.g. after an iPhone is switched on, when the screens of the iPhone and/or connected physical device are locked). This includes the following functionalities.
 - (1) Listening mode. The iOS device constantly scans for BLE advertisements from the Apple connected physical device. These advertisements are relevant to signal that an action should be executed on the iOS device;
 - (2) Establish connection. The iOS device can establish and maintain a connection between the iOS device and the Apple connected physical device at any time to transmit data between these devices;
 - (3) Network access. Apple’s iOS apps have network access on the iOS device, including to send and receive data from internet servers, for purposes related to the connected physical device.

5.6.2. *Feature falls within the scope of Article 6(7) of Regulation (EU) 2022/1925*

- (303) The Commission finds that the background execution feature as described in Section 5.6.1 of this Decision – together with its functionalities – falls within the scope of Article 6(7) of Regulation (EU) 2022/1925. The background execution feature is a hardware and software feature which is controlled via iOS, Apple’s operating systems for iPhones, which is listed in the Designation Decision.

5.6.3. *Current implementation for Apple’s own services and hardware*

- (304) The background execution feature is available to and used by Apple. Apple’s own connected physical devices, such as the Apple Watch, use background execution capabilities on iOS devices not available to third parties to exchange data with the iOS device.
- (305) [...] ³³¹
- (306) The Apple Watch iOS app facilitates, for instance, the pairing process with an Apple Watch. ³³² [...] ³³³

³³⁰ For example, as proposed by Apple in its submission of 7 November 2024, paragraph 62.

³³¹ Apple’s reply to RFI 6 of 23 October 2024, questions 18 and 21.

³³² See <https://support.apple.com/en-gb/guide/watch/apdde4d6f98e/watchos>, accessed on 11 November 2024.

³³³ Apple’s reply to RFI 7 of 14 November 2024, question 7; Apple’s reply to RFI 3 of 7 October 2024, question 47; Apple’s reply to RFI 4 of 14 October 2024, question 16.

- (307) Apple-only iOS background execution refers to the capabilities of iOS devices to exchange data and execute actions in the background with respect to Apple connected physical devices. [Many of these capabilities are enabled by processes that run continuously in the background without user interaction (daemons), allowing them to perform tasks even when the device is locked. Only Apple can add these long-running processes to iOS.]³³⁴ [...] ³³⁵ [...]
- (308) For example, for the Apple Watch, health data synchronization is handled by the *healthd* daemon, while internet sharing is handled by the *terminusd* daemon.³³⁶ [...] ³³⁷ [...] ³³⁸
- (309) [iOS decides when and for how long processes relating to the Apple Watch can run on iOS.]³³⁹ [The background processes relating to Apple Watch allow it to obtain runtime for its background processes without need for an explicit trigger.] Apple considers that there are no other limitations on the background execution capabilities in relation to the Apple Watch.³⁴⁰

5.6.4. *Current implementation for third-party services and hardware*

- (310) The background execution capabilities of third-party iOS apps are determined by the regular iOS background execution mechanisms and rules. Third-party iOS apps cannot benefit from the Apple-only iOS background execution.
- (311) Third-party manufacturers of connected physical devices often offer iOS companion apps for their devices.³⁴¹ Similarly, third-party developers of apps for connected physical devices offer iOS sister apps which are designed to communicate with the same app on a connected physical device to, for instance, keep fitness statistics in both apps synchronised. Companion and sister apps often enable functionalities regarding the third-party connected physical device that rely on regular iOS background execution; by contrast, for the same or similar functionalities, the Apple Watch relies on Apple-only iOS background execution. As a result, the third-party smartwatch may not receive certain data in time, as the rules applied to regular iOS background execution or its implementation impose restrictions that may not allow the necessary runtime at the time when it is needed. For instance, the smartwatch provider may use the companion app to download information from internet servers (e.g. news or weather updates) and transmit this information to the smartwatch via Bluetooth. Differences in background execution capabilities may lead to delays in providing up-to-date information on the third-party smartwatch, which do not affect Apple's services and hardware, such as the Apple Watch.

³³⁴ Apple's reply to RFI 4 of 14 October 2024, question 16.

³³⁵ Apple's reply to RFI 4 of 14 October 2024, question 16.

³³⁶ Rollshausen et al., "WatchWitch: Interoperability, Privacy, and Autonomy for the Apple Watch," Proceedings on Privacy Enhancing Technologies, volume 2025, pages 4 and 6.

³³⁷ Apple's reply to RFI 4 of 14 October 2024, question 22.

³³⁸ Apple's reply to RFI 4 of 14 October 2024, question 17.

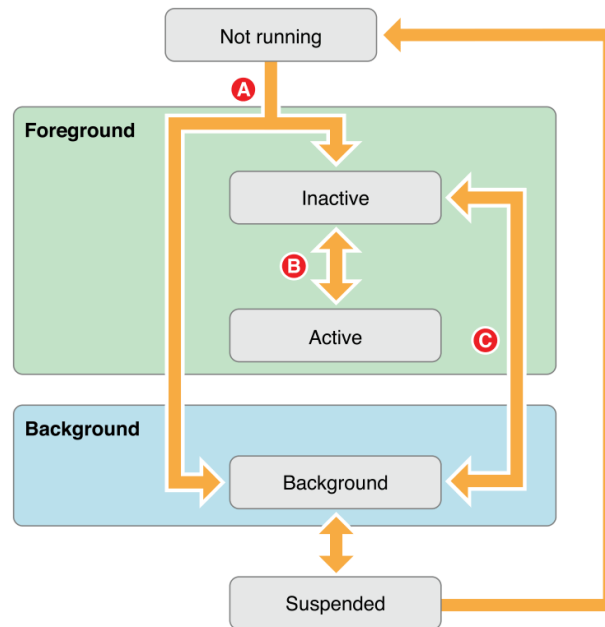
³³⁹ Apple's reply to RFI 4 of 14 October 2024, question 16.

³⁴⁰ Apple's reply to RFI 4 of 14 October 2024, question 16.

³⁴¹ For the avoidance of doubt, the use of a companion app is not always necessary in order to pair any third-party connected physical device to an iPhone (e.g. headphones). However, third parties require companion apps to offer certain functionalities (e.g. customisation) on a third-party connected physical device that are available to Apple connected physical devices without a companion app. For example, the Jabra Sound+ app or Bose Connect app, see <https://www.jabra.com/software-and-services/apps/jabra-sound-plus>, and <https://www.bose.com/apps/bose-connect>, both accessed on 11 November [2024].

- (312) The regular iOS background execution rules applicable to iOS apps govern the allocation of system resources (e.g. CPU, memory) to these apps.³⁴² The precise rules for such allocation are not transparent, and they depend on the state of the companion or sister app. According to Apple, an iOS app, such as a companion or sister app, can be in five states, namely not running, inactive, active, in the background, or suspended (see Figure 9).

Figure 9: Schematic overview of the various phases and states of running apps



Source: https://developer.apple.com/documentation/watchkit/life_cycles/handling_common_state_transitions, accessed on 11 November 2024.

- (313) A companion or sister app can be “active” in the foreground (e.g. directly after launching an app) or in the “background” (i.e. when an app is no longer in the foreground).³⁴³ An app that runs in the foreground can typically execute actions such as accessing information from the internet, playing music, tracking location, or saving photos. For apps that are in the background, iOS significantly restricts the ability to execute actions.
- (314) According to Apple’s developer documentation, iOS supports 13 background execution modes for third-party apps, enabling background execution to some extent for, *inter alia*, playing audible content in the background, location updates, communicating with an accessory, or fetching new content from a network.³⁴⁴ Some of these background execution modes are meant for interacting with a third-party connected physical device, such as the “Uses Bluetooth LE accessories”, “Users Nearby Interaction,” or “External accessory communication” modes.
- (315) iOS may also suspend or terminate an app that runs in the background, meaning that the app can no longer execute any actions. iOS may do this for several reasons, including to avoid battery drain. Apps that are suspended can be brought to

³⁴² Apple’s reply to RFI 6 of 23 October 2024, question 17.

³⁴³ Apple’s reply to RFI 4 of 14 October 2024, question 4.

³⁴⁴ See <https://developer.apple.com/documentation/xcode/configuring-background-execution-modes>, accessed on 16 September 2024.

foreground or background (possibly without user interaction) with the ability to execute code continuing from the state before suspension.³⁴⁵ Generally, a terminated app can only be moved to the foreground when a user explicitly re-opens the app, in which case the app restarts from a clean state without the ability to continue from the previous.³⁴⁶

- (316) The availability of sufficient runtime for a companion or sister app to offer functionalities to third-party connected physical devices depends on the complex interplay of whether an app is merely suspended, as opposed to terminated by iOS, whether the third-party connected physical device can send a BLE trigger signals to unsuspend the companion app, and whether iOS grants the companion or sister app sufficient runtime.
- (317) For instance, if a smartwatch companion app is in a suspended state,³⁴⁷ Apple explained that third-party smartwatches connected to an iOS device via BLE have the ability to obtain sufficient runtime for the smartwatch companion app. In technical terms, the smartwatch must send a BLE advertisement to the iOS device, upon which iOS allows the third-party smartwatch companion app to execute code during a [time window. T]he actual window during which iOS allows the companion app to execute actions depends on system load.³⁴⁸ This means that the companion app may not have any ability to execute code, or may have it for less [time].
- (318) [...] Importantly, iOS terminates the companion or sister app if a user swipes it up in the app switcher menu of an iOS device (so-called “force-quitting” or “force-killing” of an app). Users may do so for several reasons, and iOS does not inform users that this terminates the companion or sister app and results in the companion or sister app no longer being able to execute actions upon receiving a BLE advertisement (see Figure 10).³⁴⁹ Moreover, iOS will immediately disconnect from third-party Wi-Fi and Bluetooth connected physical devices when the user toggles the Wi-Fi or Bluetooth buttons in Control Centre, while several Apple services and hardware – including the Apple Watch – will continue to be available.

³⁴⁵ iOS retains the memory pages for a suspended app and restores those pages upon bringing the app back to the foreground or background. See Apple’s reply to RFI 6 of 23 October 2024, question 14.

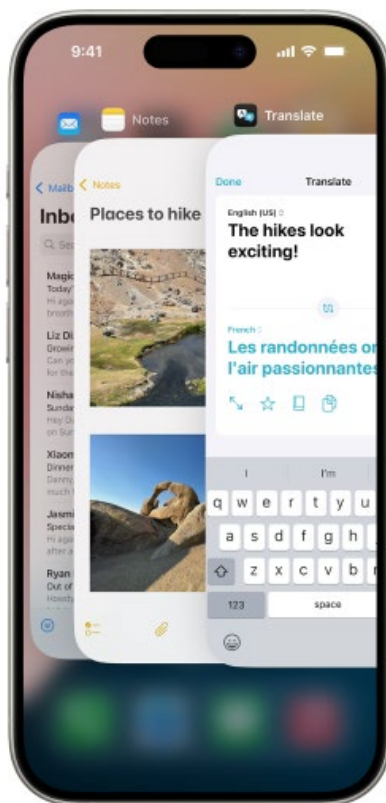
³⁴⁶ iOS discards and reclaims the memory pages for an app if it is terminated. See Apple’s reply to RFI 4 of 14 October 2024, question 8; Apple’s reply to RFI 6 of 23 October 2024, question 16.

³⁴⁷ Apple’s reply to RFI 3 of 7 October 2024, question 46; Apple’s reply to RFI 4 of 14 October 2024, question 10.

³⁴⁸ Apple’s reply to RFI 4 of 14 October 2024, questions 5 and 9.

³⁴⁹ Apple’s reply to RFI 6 of 23 October 2024, question 19.

Figure 10: Switcher menu on an iOS device



Source: <https://support.apple.com/en-ca/guide/iphone/iph1a1f981ad/ios>, accessed on 6 November 2024.

- (319) In summary, third-party connected physical devices rely on companion and sister apps to enable the use of that connected physical device and to control its functionalities, which are subject to the aforementioned background execution restrictions (the regular iOS background execution rules). In contrast, the Apple Watch can rely on privileged iOS background processes (the Apple-only iOS background execution rules) that are only available to Apple and that are not subject to the app execution restrictions, giving the Apple Watch an advantage in terms of, e.g. the reliability of the Bluetooth connection or timely data updates.
- (320) Therefore, the Commission considers that there is currently an interoperability gap when it comes to third-party connected physical devices connected to iOS devices and that it should specify how Apple has to fill this gap to comply with Article 6(7) of Regulation (EU) 2022/1925.

5.6.5. *The gatekeeper's view*

- (321) Apple considers that the measures described in the Preliminary Findings in relation to the background execution feature exceed the requirements of Article 6(7) of Regulation (EU) 2022/1925.³⁵⁰
- (322) *In the first place*, Apple argues that background execution is not a hardware or software feature within the meaning of Article 6(7) of Regulation (EU) 2022/1925. Instead, Apple argues that background execution is a reference to various aspects of

³⁵⁰ Apple's reply to Preliminary Findings, paragraph 130.

running apps in the background, which encompasses multiple aspects of app operation.³⁵¹

- (323) *In the second place*, Apple argues that requiring Apple to provide the same background execution capabilities is not necessary to achieve effective interoperability and would be disproportionate.³⁵² *First*, Apple claims that, while it is true that there are differences between user limitations for Apple’s own connected physical devices and third-party devices, these do not impact the usability or (inter)operability of said third-party devices.³⁵³ Apple argues that there is no evidence that providing the same capabilities for companion apps would be suitable to achieve contestability, and that the lack of requests for equal background execution capabilities by third parties means that such capabilities are not required to allow them to develop competing offerings. Apple considers that the existence of third-party physical connected physical devices that function shows that background runtime differences do not hinder the operation of connected physical devices and companion apps.³⁵⁴ *Second*, Apple argues that Article 6(7) of Regulation (EU) 2022/1925 does not require Apple’s interoperability solutions to provide parity of limitations of background execution capabilities as between Apple’s own connected physical devices and third-party connected physical devices. *Third*, Apple considers that Article 6(7) of Regulation (EU) 2022/1925 does not require to ensure equality of end user choice between Apple’s and third-party services, including in cases where Apple were to present end users with such a choice.³⁵⁵
- (324) *In the third place*, Apple argues that granting unfettered access to hardware or software functionalities to apps that run in the background would raise significant integrity concerns, including unexpected significant battery drain and harm to device performance. Apple argues that Apple does not need to impose the same restrictions on its own services and hardware because those can, and do, choose to use the iOS resources responsibly. Apple considers that third parties do not have the same incentive as Apple’s connected physical devices to use resources responsibly because they are not held accountable for the performance of iOS as a whole.³⁵⁶
- (325) *In the fourth place*, Apple argues that introducing new background execution processes requires careful developing, engineering, and testing, particularly due to the wide range of connected physical devices to support. [...] ³⁵⁷

5.6.6. Commission’s assessment

- (326) The Commission notes that in some points of its response to the Preliminary Findings, Apple refers to the background execution feature as “*Bluetooth background execution*.”³⁵⁸ The Commission notes that the Preliminary Findings do not use this expression and in fact do not restrict the feature to Bluetooth communication or to data transmission. First, the description of the feature is not limited to Bluetooth as a communication technology – see Section 5.6.1 of this Decision. Second, the description of the feature explicitly includes the ability to

³⁵¹ Apple’s reply to Preliminary Findings, Section VII.B.b.

³⁵² Apple’s reply to Preliminary Findings, Section VII.B.c.

³⁵³ Apple’s reply to Preliminary Findings, paragraph 157.

³⁵⁴ Apple’s reply to Preliminary Findings, paragraph 147.

³⁵⁵ Apple’s reply to Preliminary Findings, paragraphs 158-164.

³⁵⁶ Apple’s reply to Preliminary Findings, paragraph 151.

³⁵⁷ Apple’s reply to Preliminary Findings, Section VII.B.d.

³⁵⁸ See, for example, Apple’s reply to Preliminary Findings, paragraph 129.

communicate with *and* execute actions on an iOS device, mentioning in particular the allocation of system resources such as CPU and the allocation of runtime – see recital (295) of this Decision. The examples in recital (291) of this Decision also clearly go beyond mere transmission of data, as they require to perform operations on the iOS device. The importance of performing operations in the background was also confirmed by [third-party developer] in its response to the Preliminary Findings, for example for operations such as processing of photos and execution of AI models.³⁵⁹ As such, the feature was and remains background execution, not “Bluetooth background execution.”

5.6.6.1. Concerning the claim that background execution is not a feature

- (327) Background execution is a feature without which connected physical devices and related apps would not function properly. It is a fundamental feature that the operating system makes available to ensure apps can function as intended by the developer and end user. That is why Apple currently makes a certain level of background execution available to all apps and connected physical devices, including to play audio, provide location updates, enable calls, enable push notifications and communicate with connected physical devices. The importance of background execution is confirmed by the fact that Apple comprehensively explains to app developers in its developer documentation how to make effective use of the background execution feature.³⁶⁰ During its annual developer conference Apple explains how to make use of this feature and describes that “*background execution is a powerful tool your app can leverage to provide a great user experience.*”³⁶¹ Apple also refers to it as a “*capability*” that developers can add to their app.³⁶²
- (328) Market participants and developers of apps and connected physical devices clearly consider background execution an iOS feature [Third-party developer] filed an interoperability request specifically for background execution.³⁶³ [Third-party developer] asked for access to background execution during the specification proceedings.³⁶⁴ Two other developers filed requests concerning background execution with Apple, stating that “*users expect the syncing to happen in the background, but third-party apps have to rely on background time to sync new assets, which is unreliable for two main reasons*”³⁶⁵ and requesting to “*hav[e]*

³⁵⁹ [Third-party developer]’s submission to the public consultation, paragraph 15(a).

³⁶⁰ See <https://developer.apple.com/documentation/uikit/using-background-tasks-to-update-your-app>, <https://developer.apple.com/documentation/uikit/extending-your-app-s-background-execution-time>, <https://developer.apple.com/documentation/uikit/about-the-background-execution-sequence>, <https://developer.apple.com/documentation/xcode/configuring-background-execution-modes>, all accessed on 24 February 2025.

³⁶¹ See <https://developer.apple.com/videos/play/wwdc2019/707/>, accessed on 24 February 2025.

³⁶² See <https://developer.apple.com/documentation/xcode/configuring-background-execution-modes>, accessed on 24 February 2025.

³⁶³ [Third-party developer] interoperability request submitted to Apple on 19 January 2024, see list of all interoperability requests Apple received until 31 January 2025 in Apple’s reply to RFI 11 of 28 November 2024.

³⁶⁴ See e.g. [third-party developer]’s submission of 29 January 2025.

³⁶⁵ See interop request [...] submitted to Apple on 26 January 2024 by [third-party developer], see list of all interoperability requests Apple received until 31 January 2025 in Apple’s reply to RFI 11 of 28 November 2024.

See e.g. [third-party developer]’s submission of 29 January 2025.

periodic background time available to our app.”³⁶⁶ During the public consultation, several respondents expressed support for the measures proposed by the Commission in relation to background execution, with one third party defining it a “*high-impact feature*”.³⁶⁷

- (329) Apple’s claim that background execution is not necessary to offer specific functionalities to end users is wrong.³⁶⁸ As [third-party developer] explained, without background execution, important updates would not be shown on a [third-party developer] watch, which negatively affects end users.

5.6.6.2. Concerning effective interoperability and proportionality

- (330) *First*, as explained in Section 3.1.1 of this Decision, the Commission is not required to demonstrate that each of the measures are necessary to enable contestability, i.e. that (some) third parties are able to provide a “*competitive offering*” or an “*alternative solution*” which is enough for achieving contestability.³⁶⁹ Such assessment would re-import the effects analysis, which the legislator explicitly rejected and is contrary to the text and purpose of Article 6(7) of Regulation (EU) 2022/1925 – see also recital (77)(e) of this Decision. Apple claims: “*Currently, third-party physical connected devices function, which shows that any possible background runtime differences do not hinder the operation of connected physical devices and companion apps on iOS.*”³⁷⁰ Article 6(7) of Regulation (EU) 2022/1925 aims at creating a level playing field as regards access to iOS features; merely allowing third party devices to “*function*” is insufficient.
- (331) *Second*, [...].³⁷¹ As explained in recital (328) of this Decision, there is clear demand for this feature, as evident from the third parties who submitted requests in relation to background execution, including [third-party developer]’s request in the context of connected physical devices.
- (332) *Third*, the fact that third-party devices exist despite the current interoperability gap obviously does not imply that there is effective interoperability: a service can in principle exist even if it is at a disadvantage in terms of interoperability, as is the case for the background execution feature.
- (333) *Fourth*, if the current interoperability gap was materially insignificant as argued by Apple, Apple could easily comply with the measures by simply applying the same existing limits to its own services and hardware. Instead, Apple goes to great lengths to explain why it should not be subject to equal conditions with third parties for access to the background execution feature.

5.6.6.3. Concerning integrity

- (334) *First*, Apple does not raise integrity concerns regarding the feasibility of building an interoperability solution, i.e. that Apple cannot technically implement the feature. Its

³⁶⁶ See interop request [...] submitted to Apple on 25 January 2024 by [third-party developer], see list of all interoperability requests Apple received until 31 January 2025 in Apple’s reply to RFI 11 of 28 November 2024.

See e.g. [third-party developer]’s submission of 29 January 2025.

³⁶⁷ [Third-party developer]’s submission to the public consultation, page 1.

³⁶⁸ Apple’s reply to Preliminary Findings, paragraph 138.

³⁶⁹ See Section 3.1.1 of this Decision.

³⁷⁰ Apple’s reply to Preliminary Findings, paragraph 147.

³⁷¹ Apple’s reply to Preliminary Findings, paragraph 157. See also Apple’s internal document [...].

concerns should thus be limited to the implementation phase, i.e. the adjustments under which that solution is made available to third parties.³⁷²

- (335) *Second*, as outlined in Section 3.3 of this Decision, Apple fails to duly justify the measures it intends to take to mitigate integrity risks as necessary and proportionate in the context of implementing effective interoperability. Apple merely assumes that the measures would require granting third parties “*unfettered access*” to background execution. Such a level of background execution is not required by the measures in this Decision, nor was it included in the Preliminary Findings or the Draft Final Measures. Instead, the Commission consistently required that Apple grants the same level of background execution to third parties as Apple grants its own services or hardware. Apple therefore justifies integrity concerns against a non-existing obligation, which is much stricter than the actual obligation. It is not clear whether Apple has concerns regarding the actual measure, what these concerns would be, and what an appropriate mitigating measure would be.
- (336) Under the measures in this Decision, the Preliminary Findings, and the Draft Final Measures, Apple is not precluded from applying rules to prevent undue impact on the battery usage, provided the rules are transparent, objective, precise and non-discriminatory, applying also to Apple’s services and hardware. This allows Apple to define the conditions of interoperability with the feature, while ensuring that Apple does not grant itself more favourable conditions and ensuring that the rules do not discriminate against certain third parties or use cases.
- (337) Apple’s proposed mitigating measure is also not duly justified because it is unclear. [...] ³⁷³ [...] ³⁷⁴ [...]
- (338) *Third*, Apple’s proposed mitigating measure is neither strictly necessary nor proportionate. Under its proposal, Apple would be the arbiter on what runtime is “*sufficient*” and what use cases are supported, which would be contrary to the purpose of Article 6(7) of Regulation (EU) 2022/1925. Apple does not comment on the proportionality of its proposal. Instead, the Commission considers that an alternative proportionate mitigating measure could be to ask the end user what level of background execution each device should enjoy. Allowing the user to make an informed decision about which connected physical devices and related apps – both from Apple and third parties – should be permitted to consume most battery life would enable end users to make use of innovative connected physical devices and allow third parties to enjoy interoperability under the same conditions as Apple. Battery consumption is an important parameter of competition. For example, if a certain app uses more battery than a competing app, the end user can consider this aspect when renewing the subscription for the app. Apple already provides the end user with information on the battery usage of apps in iOS settings, including for background activity, and allows the user to limit it (Figure 11).³⁷⁵

³⁷² Agreed minutes of the meeting with Apple of 11 and 12 February 2025.

³⁷³ Apple’s mark-up of the Commission’s proposed measures of 23 January 2025.

³⁷⁴ Apple’s mark-up of the Commission’s proposed measures of 23 January 2025.

³⁷⁵ See <https://support.apple.com/en-us/120745> accessed on 24 February 2025: “*Battery Usage by App displays a list of apps that have used the battery as well as the proportion of the battery that each app used. Tap the app to see its onscreen and background usage times. You can improve battery life by reducing your use of the app that has used the most battery.*”

Figure 11: Battery and background activity information made available in iOS settings

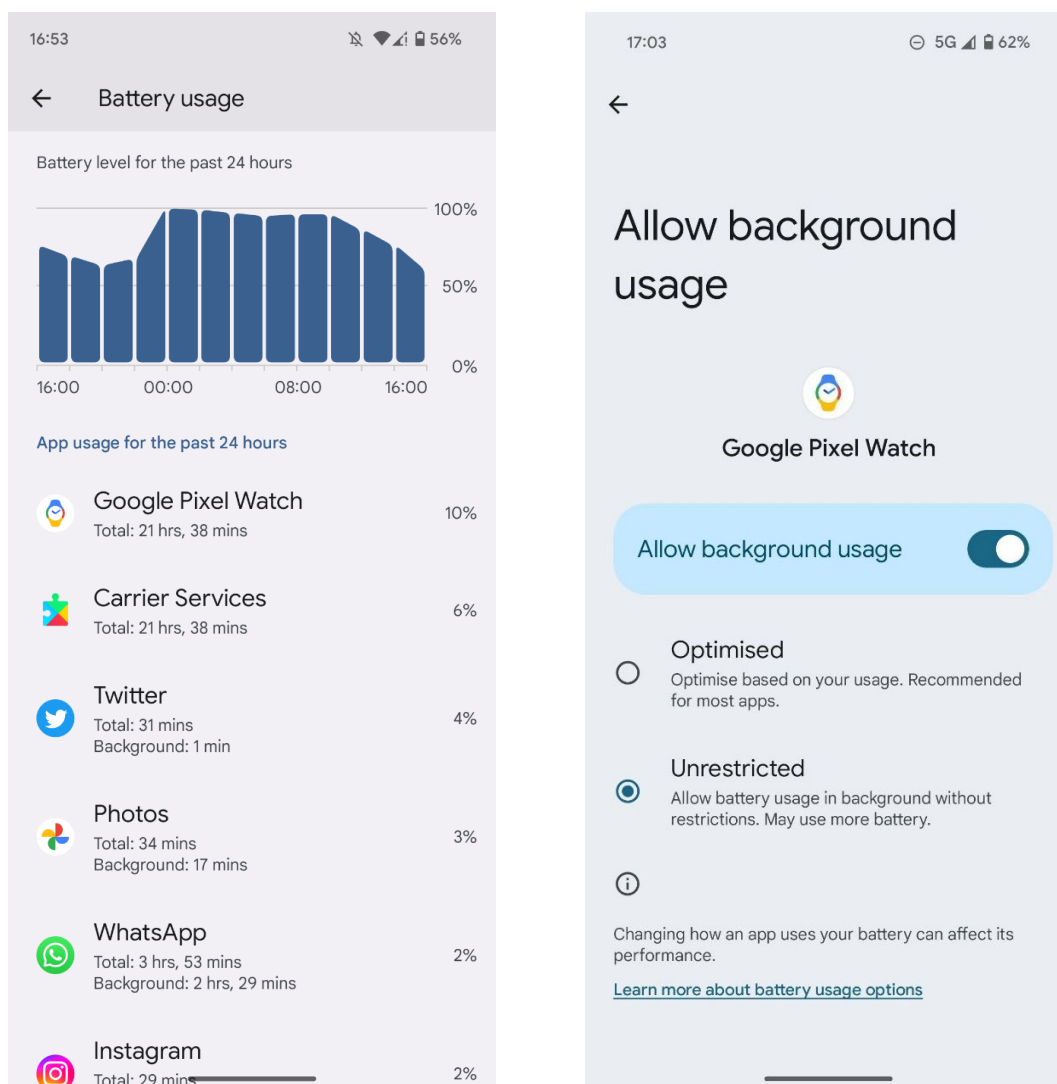


Source: screenshot from iOS device taken by Commission.

- (339) Apple can continue to show this information in a neutral and non-discriminatory manner, including with respect to connected physical devices, thus allowing end users to make an informed decision about which connected physical devices and apps to use. This measure would be less restrictive than Apple's proposal and would ensure equal conditions and user choice. [...] ³⁷⁶ Moreover, the information and options provided to users on smartphones running Android – Google's operating system – shows that an approach based on transparency to the user and user agency is possible. Smartphones running the Android operating system show the background time used by any app and allow the user to set the desired level of background execution for any app, including apps relating to Google's connected physical devices (Figure 12, see entry "Google Pixel Watch").

³⁷⁶ Apple's reply to Preliminary Findings, paragraph 163.

Figure 12: Battery usage overview and settings on an Android smartphone, showing battery usage for the Google Pixel Watch and allowing the user to choose the desired background usage



Source: <https://www.reddit.com/media?url=https%3A%2F%2Fi.redd.it%2Fqp6warqvl6v91.png>, accessed on 20 February 2025.

- (340) *Fourth*, in any case, Apple does not substantiate the existence of an integrity concern. The purpose of an iOS device's battery is to power the use of an iOS device according to the user's preferences. Apple does not currently limit users in using the iPhone's battery even for power-intensive use cases such as gaming and watching videos, explaining that "*it's normal for some apps to use a large portion of battery.*"³⁷⁷ Moreover, if a user takes videos via a connected physical device and uses functionality in the companion app to process this video on the iOS device when the app is in the background, this does not impair the functioning of iOS or of background execution in itself. Apple may apply rules that prevent unexpectedly high battery usage under certain conditions, in a non-discriminatory way.

³⁷⁷ See <https://support.apple.com/en-us/120745>, accessed on 24 February 2025: "*It's normal for some apps to use a large portion of battery. For example, graphics-intensive or processor-intensive apps or games that stream high-quality video often use more battery than other apps.*"

- (341) It is therefore unclear why Apple considers that access to background execution under equal conditions – including by enabling user agency if Apple so chooses – could compromise integrity. A mitigating measure based on user agency allows Apple not to reserve sufficient runtime for other system-relevant iOS processes or apps. Considering Android’s experience with its mobile operating system, it appears that it is possible to mitigate Apple’s concerns in relation to battery life via user agency. Android allows users to grant each app unrestricted (allow all background work), optimized (by default, background runtime depends on how the user interacts with the app) or restricted (no background execution) background execution (Figure 12).³⁷⁸ Apple therefore has not properly substantiated the existence of an integrity concern.
- (342) Fifth, Apple proposes measures to mitigate integrity concerns which would not be proportionate. Apple argues [third parties have different incentives regarding the responsible use of iOS resources than Apple itself, that is held accountable for its services and hardware.]³⁷⁹ [...]. As explained in Section 3.3 of this Decision, Apple may take integrity measures based on transparent, objective, precise and non-discriminatory conditions that apply to Apple and third parties. Apple’s claims do not meet this test. “Responsible” use of iOS resources is neither objective nor precise. This condition is also not capable of being independently verified, and it is intrinsically liable to affect third parties more than Apple because it is based on Apple’s general assumptions about the incentives of third parties and on Apple’s trust for its own services and hardware.

5.6.6.4. Concerning sister apps

- (343) For the purpose of this Decision, an iOS sister app is an iOS app that is designed to communicate with the same app on a connected physical device.³⁸⁰ The Preliminary Findings found that there is a gap between third-party connected physical devices and Apple’s devices in terms of background execution for iOS sister apps.³⁸¹ Apple did not dispute these findings.
- (344) Sister apps may be provided by third parties that are not the provider of the connected physical device. Apple supports third-party apps on the Apple Watch, including sister apps that have a corresponding iOS sister app.³⁸² Like the Apple Watch, third-party connected physical devices may also operate as platforms that support the installation and use of third-party apps. For example, [third-party developer] supports third-party apps on some of its smartwatches, such as fitness apps. Those apps can currently communicate with their iOS sister apps,³⁸³ meaning

³⁷⁸ See <https://developer.android.com/topic/performance/background-optimization> accessed on 24 February 2025.

³⁷⁹ Apple’s reply to the Preliminary Findings, paragraph 151.

³⁸⁰ See recital (138) of this Decision.

³⁸¹ Apple’s reply to the Preliminary Findings, paragraph 171.

³⁸² This is supported by the *WatchConnectivity* and *WatchKit* frameworks, cf. Apple’s reply to RFI 2 of 30 September 2024, Annex 1.2, point 1(vi); and Agreed minutes of meeting with [third-party developer] of 29 October 2024, paragraph 2. Apple uses the expression “companion app” to refer to these apps, see: <https://developer.apple.com/watchos/planning/>, accessed on 24 February 2025. To avoid confusion with apps that facilitate the use of the connected physical device, this Decision intentionally distinguishes between companion apps and sister apps – see recitals (137)-(138) of this Decision.

³⁸³ Agreed minutes of meeting with [third-party developer] on 3 February 2025.

that the installation and use of sister apps on third-party connected physical devices is already possible on iOS today.³⁸⁴

- (345) Measures for the background execution feature cover not only companion apps, but sister apps as well – see Section 5.6.7 of this Decision. Those measures aim at ensuring that access to the background execution feature is not restricted to the companion app or to the provider of the connected physical device, but rather extends to every iOS app that is designed to communicate with the same app on a connected physical device. This capability is necessary for several use cases (see examples in recital (291) of this Decision), which rely on the iOS app’s ability to communicate and execute actions in the background. Apple already allows sister app to function on iOS devices with respect to third-party connected physical devices. The measures in this Decision merely seek to ensure that the iOS sister apps have access to the same background execution feature as Apple in an equally effective way.
- (346) Apple raised in an email sent after the deadline to respond to the Preliminary Findings had elapsed that, [Apple has security concerns].³⁸⁵ On the same day, the Commission organised a meeting with Apple to discuss this matter. Apple explained to the Commission that it was concerned that [...] Apple informed the Commission that it was investigating whether such a security design flaw exists in iOS. Third parties contradicted Apple’s concerns, explaining that [...] Apple did not communicate to the Commission the result of its investigation and did not raise the topic again during the proceedings.
- (347) The Commission considers that Apple’s claims regarding the potential security risks of sister apps are not substantiated. Apple has not claimed that its concerns would relate to the integrity of iOS or the background execution feature, nor has Apple showed that the security design flaw does in fact exist. In any case, this Decision clarifies that the measures on background execution in the Annex to this Decision do not require Apple to remove existing user permission prompts for Bluetooth access. The Commission also notes that the Draft Final Measures – including measures for background execution – were shared with Apple on 7 February 2025 and Apple did not raise any point relating to sister apps since then.

5.6.6.5. Concerning timing

- (348) Apple has had a significant amount of time to consider and work on an interoperability solution for the background execution feature. Apple received the first formal requests for interoperability with the background execution feature in January 2024.³⁸⁷
- (349) In their response to the Preliminary Findings, Apple indicated the wide range of connected physical devices as a reason why implementing interoperability with the

³⁸⁴ Connected physical devices can also support third-party iOS apps without the need to have the same app installed on the connected physical device. For example, the iOS Be My Eyes app is not provided by [third-party developer], but can interoperate with the [third-party developer’s connected physical devices], accessing the [connected physical devices]’ camera in order to provide assistance to blind or low vision end users. See agreed minutes of meeting with [third-party developer] on 3 February 2025.

³⁸⁵ Email from Apple to the Commission on 3 February 2025 –[on background execution].”

³⁸⁶ Agreed minutes of meeting with [third-party developer] on 3 February 2025; Agreed minutes of meeting with [third-party developer] on 3 February 2025. The minutes of these meetings were provided to Apple on 5 February 2025.

³⁸⁷ See recital (121)(d) of this Decision.

background execution feature may not be possible within the timing considered by the Commission in the Preliminary Findings (i.e. the next major iOS release – expected in fall 2025, and in any case by the end of 2025). The Commission considers that the requirement to design and implement transparent, neutral and non-discriminatory rules for a wide range of devices may indeed require more time.

(350) [...] ³⁸⁸

(351) The Commission therefore considers Apple’s proposed two-step approach on timing appropriate, in light of the different technical complexity of the two parts of the feature. Therefore, Apple should implement the measures concerning background execution for third-party companion apps in relation to force-quitting and Bluetooth/Wi-Fi disabling actions in the next major iOS release, i.e. iOS 19, and in any case by the end of 2025 at the latest, and all of the measures for the background execution feature in the release of iOS 20, and in any case by the end of 2026 at the latest.

5.6.7. *Measures that Apple should implement*

(352) To meet the requirements of Article 6(7) of Regulation (EU) 2022/1925, Apple should implement an interoperability solution that provides third parties with access to the same background execution feature as available to Apple (as described in Section 5.6.1 of this Decision), in a way that is equally effective as the solution available to Apple.

(353) Apple should provide interoperability with all functionalities of the background execution feature which are available to Apple’s own connected physical devices, including, but not limited to, AirPods, Apple Vision Pro, Apple Watch, as well as any future Apple connected physical devices. Apple should provide interoperability with the following functionalities.

- (a) Apple should grant iOS companion apps, iOS sister apps, and relevant iOS processes the same background execution capabilities on iOS devices to execute actions with respect to third-party connected physical devices that Apple grants, including via iOS processes and iOS daemons, to execute actions with respect to Apple’s connected physical devices. This includes any restrictions, time windows, and resource limitations (e.g. on CPU and/or GPU execution), which Apple should apply according to transparent, objective, precise and non-discriminatory rules that also apply to Apple’s services and hardware, including for use cases that Apple does not offer. ³⁸⁹

³⁸⁸ Email from Apple to the Commission of 3 February 2025.

³⁸⁹ The rules governing background execution should not be discriminatory towards third-party connected physical devices and related apps. For example, users can activate Siri directly from the Apple AirPods and ask the virtual assistant to perform some tasks, even when the iPhone’s screen is off (see <https://support.apple.com/guide/airpods/use-siri-devc2c0f438a/web>, accessed on 24 February 2025). Apple should not discriminate against third-party voice assistants with respect to third-party connected physical devices. That includes future Apple connected physical devices with more advanced functionality ([...]). In particular, to ensure that innovation is not undermined, the rules should not be discriminatory as regards allocating sufficient background execution capabilities to innovative connected physical devices and relates apps. Apple should enable such innovation in a non-discriminatory way even if Apple does not (yet) offer that specific type of connected physical devices – such as bike computers – or functionality (e.g. a third-party voice assistant implements more functionality than Siri does).

- (b) Any limitation or choice on the background execution capabilities of third-party iOS companion apps, iOS sister apps, or relevant iOS processes with respect to third-party connected physical devices as a result of a user action should only be permissible if the user can take the same action with the same limiting effect regarding Apple's most comparable connected physical devices. This includes the action of a user terminating a companion or sister app in the app switching menu ("force-quitting") and the action of disabling Wi-Fi or Bluetooth through iOS Control Centre, as well as the resulting impact on background execution with the connected physical device.
 - (c) Apple should grant third-party iOS companion apps or iOS sister apps equal use of background execution functionalities – regardless of whether an active end user interaction took place³⁹⁰ – under transparent, objective, precise, and non-discriminatory rules that also apply to Apple's services and hardware, including for use cases that Apple does not offer. These functionalities include:
 - (1) having the iOS device constantly listen for signals from the third-party connected physical device based on BLE and any other communication protocol that Apple uses to scan for advertisements from a connected physical device;
 - (2) allowing the iOS companion app or iOS sister app to timely establish, maintain and use a connection between the iOS device and the third-party connected physical device to transmit data between the app and the third-party connected physical device; and
 - (3) allowing the iOS companion app and iOS sister app network access on the iOS device, including to send and receive data from internet servers, for purposes related to the connected physical device.
- (354) Apple may continue to require user permission for Bluetooth access APIs that currently require such user permission in compliance with the requirements of Article 6(7) of Regulation (EU) 2022/1925.³⁹¹
- (355) Apple should grant third parties access to additional functionalities if necessary to enable effective interoperability with the background execution feature referred to in recital (352) of this Decision.
- (356) Apple shall also provide effective interoperability with any future updates, including new functionalities, of the background execution feature insofar as they are available to Apple's own connected physical devices. To this end, the general measures in Section 5.12 of this Decision apply, including in particular the measures concerning future updates and new functionalities set out in Section 5.12.7 in this Decision.

5.6.8. *Implementation timing*

- (357) Apple should implement the measures to provide effective interoperability with the background execution feature for third-party companion apps in relation to force-quitting and Bluetooth/Wi-Fi disabling actions in the next major iOS release, i.e. iOS 19, and in any case by the end of 2025 at the latest, and all of the measures for the

³⁹⁰ For example, after an iPhone is switched on or when the screens of the iPhone and/or connected physical device are locked.

³⁹¹ This measure concerns Apple's security concerns described in Section 5.6.6.4 of this Decision.

background execution feature in the release of iOS 20, and in any case by the end of 2026 at the latest.

5.7. Measures for close-range wireless file transfer

- (358) Features for close-range wireless file transfer solutions, such as Apple's AirDrop, allow iPhone users to wirelessly send and receive files from other Apple connected physical devices. For example, an end user can use AirDrop on their iPhone to easily and quickly receive a photo from a friend's iPad. AirDrop is pre-installed on iOS devices and only Apple's connected physical devices can interoperate with AirDrop on an iOS device.
- (359) Apple's close-range wireless file transfer solutions, such as AirDrop, have access to iOS features such as a user interface with activity views (e.g. the iOS Share Sheet), the ability of third-party connected physical devices to discover nearby iPhones, the ability to only show those devices associated to entries in the iPhone user's contact list, the ability to transfer files using high-performance protocols and in the background, or the ability to have received files appear in relevant apps.
- (360) Third-party developers do not enjoy the same level of interoperability for their close-range wireless file transfer solutions that Apple's services and hardware enjoy. This means that third-party close-range wireless file transfer solutions do not have access to relevant features in the same way as Apple's solutions (including features used by AirDrop) do. Since Apple reserves access to certain iOS features for its own services and hardware, a level playing field is prevented. Third-party developers therefore need access to the features available to Apple's services and hardware, such as AirDrop, which is an example of a close-range wireless file transfer solution.

5.7.1. Description of the features

- (361) Offering close-range wireless file transfer solutions on iOS devices requires access to the same iOS features as available to Apple's services or hardware, including via AirDrop, regarding close-range wireless file sharing across devices.
- (362) iOS devices are capable of transferring files (or more generally "items"), such as photos, URLs, or documents, between nearby Apple devices, such as between iPhones, iPads, Mac computers, Apple Vision Pros, and Apple Watches, using close-range wireless file transfer solutions, such as AirDrop.³⁹² AirDrop is pre-installed on iOS devices (as well as on other Apple devices with their respective operating systems) and cannot be uninstalled by the end user.³⁹³ Instead, an end user can disable AirDrop through the Screen Time settings.³⁹⁴
- (363) Features for close-range wireless file transfer solutions are important for third-party developers to ensure that their solutions have access to, for example, the same communication protocols, device discovery mechanisms, and access points that are available to Apple's services and hardware, including via AirDrop.

³⁹² See <https://support.apple.com/en-gb/guide/iphone/iphcd8b9f0af/ios>, accessed on 16 September 2024; Apple's reply to RFI 7 of 8 November 2024, question 1 and Apple's internal document [...].

³⁹³ Apple's reply to RFI 6 of 23 October 2024, questions 54, 55 and 58.

³⁹⁴ Apple's reply to RFI 6 of 23 October 2024, questions 58 and 59; See <https://support.apple.com/en-us/119857>, accessed on 16 September 2024, which explains that end users need to "1. Go to Settings > Screen Time. 2. Tap Content & Privacy Restrictions. 3. Tap Allowed Apps and make sure that AirDrop is turned on."

- (364) A typical functionality of a feature for a close-range wireless file transfer solution, such as AirDrop, is the ability to restrict device discovery for file sharing to trusted devices, also called “Contacts Only” mode, where only nearby devices are shown if they are mutual contacts and within the contacts database of one another or are possessed by the same user.³⁹⁵
- (365) Features and functionalities of features for third-party close-range wireless file transfer solutions which are available to Apple’s services, including Apple’s AirDrop, are listed below.
- (a) Accessibility. The ability of close-range wireless file transfer solutions to be displayed and easily accessible in Apple and third-party services and hardware on an iOS device.³⁹⁶
 - (b) Advertisement and discovery. The ability of close-range wireless file transfer solutions to use a communication protocol to discover and be discovered by nearby Apple and non-Apple devices.³⁹⁷
 - (c) Trusted devices. The ability of close-range wireless file transfer solutions to establish trust via the operating system with another device and subsequently filter incoming file transfer requests based on whether the shared file is being sent from a device that is trusted. A trusted device may be an Apple or non-Apple connected physical device.³⁹⁸
 - (d) Protocols. The ability of close-range wireless file transfer solutions to establish and use the most appropriate available connection between an iOS device and an Apple or non-Apple connected physical device via a communication protocol or via a file sharing protocol that is based on a communication protocol.³⁹⁹

³⁹⁵ Apple’s reply to RFI 5 of 16 October 2024, question 29; Technical meeting Apple/Commission of 14 October 2024, AirDrop slide deck page 3.

³⁹⁶ For instance, this may include the ability of a file transfer solution to be integrated into Apple’s user interface for activity views (e.g. iOS Share Sheet). Integration into the iOS Share Sheet facilitates the seamless activation of the file transfer service in the background. This includes initiating the relevant file transfer protocol and, if necessary, device pairing, such that the end user does not have to open the file sharing app to send a file. Similarly, the sending device is able to trigger the system user interface on the receiving device to respond to and execute the file transfer. See <https://developer.apple.com/design/human-interface-guidelines/activity-views>, accessed on 16 September 2024; <https://support.apple.com/en-us/119857>, accessed on 6 November 2024.

³⁹⁷ Communication protocols include, but are not limited to, BLE, NFC, and P2P Wi-Fi as available to Apple. See Apple’s submission on its proposed file sharing solution of 14 November 2024, paragraph 12.

³⁹⁸ Trusted devices include those associated with a contact in the destination device’s contacts, the end user’s own devices, or generally devices for which the trust is established upon the first encounter. Trust may be established explicitly, e.g. through pairing, or implicitly, e.g. bypassing pairing by pre-establishing trust for devices possessed by the user. End users are able to configure by whom a device is discoverable in the iOS settings, i.e. by no one, trusted devices, or everyone. Technical meeting Apple/Commission of 14 October 2024 [...]; Apple’s submission [...], paragraph 8; Apple’s internal document, [...].

³⁹⁹ A close-range wireless file transfer solution is capable of supporting multiple communication technologies for file transfer, meaning that they can change the communication protocol when a more suitable connection is available, for instance when another connection is faster or when devices move out of range. See Apple’s reply to RFI 3 of 7 October 2024, question 23; Apple’s reply to RFI 5 of 16 October 2024, question 34; Apple’s reply to RFI 1 of 23 September 2024, question 19; Apple’s submission [...], paragraph 8.

- (e) Background execution. The ability of close-range wireless file transfer solutions to initiate a file transfer via interfaces supported in iOS that do not require the launching of a separate app, or to execute and continue file sharing in the background if previously initiated by the end user. Any user interface displaying the progress of the file transfer shown to the end user using a third-party solution should be under equal conditions as when using an Apple solution such as AirDrop, both on the sending and the receiving device.
- (f) File context. The ability of close-range wireless file transfer solutions to launch the app from which a file was shared using a close-range wireless file transfer solution and store the file in that app, or another app appropriate for the file type in case the corresponding app is not installed on the receiving device.

5.7.2. *Feature falls within the scope of Article 6(7) of Regulation (EU) 2022/1925*

- (366) The Commission finds that the features for close-range wireless file transfer solutions fall within the scope of Article 6(7) of Regulation (EU) 2022/1925. These functionalities are hardware and software feature which are controlled via iOS, Apple's operating systems for iPhones, which is listed in the Designation Decision.

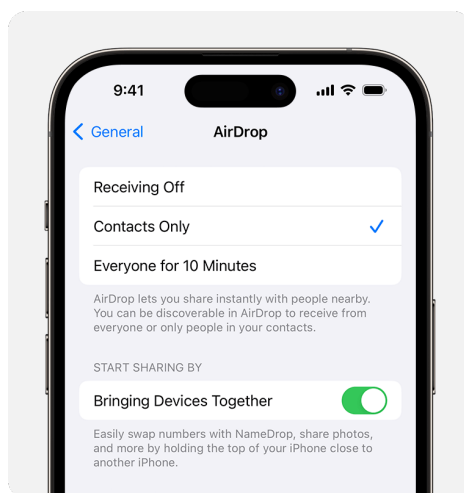
5.7.3. *Current implementation for Apple's own services and hardware*

- (367) The features for close-range wireless file transfers are used by or available to, Apple's services and hardware. For instance, Apple's close-range wireless file transfer solution AirDrop comes pre-installed on Apple devices and relies on the features for close-range wireless file transfers.
- (368) *First*, in terms of accessibility, an end user who intends to receive a file via AirDrop must ensure to have the correct settings.⁴⁰⁰ This includes having Wi-Fi and Bluetooth turned on, while the Personal Hotspot must be turned off. Furthermore, the receiving end user must activate AirDrop in the iOS settings. The AirDrop settings allow for the following three options (see Figure 13).
 - (a) Receiving off. The end user wishes to not receive files via AirDrop.
 - (b) Contacts Only mode. The end user wishes to receive files only from devices that are associated to a contact in the end user's contacts list (accessible through the iOS contacts app). This is the default setting.⁴⁰¹
 - (c) Everyone for 10 Minutes mode. The end user wishes to receive files from any nearby AirDrop-capable device, regardless of whether the device is associated to a contact in the Contacts app of the end user. After 10 minutes, the setting automatically changes to Contacts Only (if the user is signed in with their Apple Account) or Receiving off.

⁴⁰⁰ See <https://support.apple.com/en-us/119857>, accessed on 16 September 2024.

⁴⁰¹ See https://help.apple.com/pdf/security/en_GB/apple-platform-security-guide-b.pdf, page 190, accessed on 8 October 2024.

Figure 13: AirDrop device discovery settings on iOS



Source: <https://support.apple.com/en-us/119857>, accessed on 6 November 2024.

- (369) Furthermore, AirDrop, Mail, Messages and many other services of Apple have access to iOS features for better accessibility. For instance, an end user can open an app with the relevant file, tap on the Share button, and tap on the AirDrop, Mail, or Messages button in the subsequent “iOS Share Sheet” (see Figure 14). If the end user selected AirDrop, the sending device will automatically activate the AirDrop protocol.⁴⁰²

Figure 14: Share Sheet integrated into iOS apps, providing the option to share files via AirDrop



Source: <https://support.apple.com/en-us/119857>, accessed on 6 November 2024.

- (370) App developers can make files transferable to other Apple devices via AirDrop by adding sharing capabilities into their apps, which is done by integrating the iOS Share Sheet via the *UIActivityViewController* or *ShareLink* API into the iOS app.⁴⁰³

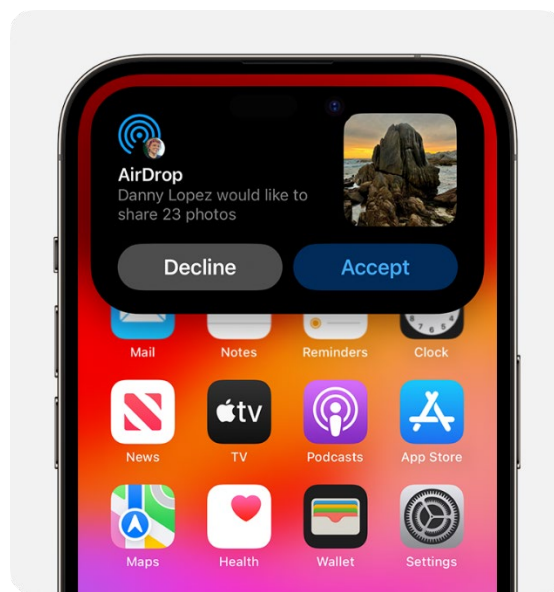
⁴⁰² Apple’s reply to RFI 5 of 16 October 2024, introduction to Section 2.2, page 13.

⁴⁰³ See <https://developer.apple.com/design/human-interface-guidelines/activity-views>, accessed on 16 September 2024 and Apple’s internal document [...].

By default, iOS will list app-specific actions that are available in multiple apps or throughout iOS in the iOS Share Sheet. The iOS Share Sheet may therefore include AirDrop, other Apple apps or services, or third-party iOS apps whose app developers configured their iOS app to appear in the iOS Share Sheet for certain types of files (e.g. a photo editor app will appear in the iOS Share Sheet when sharing a picture).⁴⁰⁴ App developers cannot modify the order in which sharing activities and actions are displayed on the iOS Share Sheet.⁴⁰⁵

- (371) Furthermore, AirDrop is capable of triggering the system user interface on the receiving Apple device in order to accept or decline the transfer (see Figure 15),⁴⁰⁶ unless the sending and destination device belong to the same user and are signed in with the same Apple Account – in which case the transfer is automatically accepted.⁴⁰⁷ Apple can enable the iOS device to “*vibrate and show a glow from the top of the display to [...] indicate that a connection is being made*” with another device in the context of an incoming transfer.⁴⁰⁸

Figure 15: User interface on receiving device for incoming AirDrop transfer



Source: <https://support.apple.com/en-us/119857>, accessed on 6 November 2024.

- (372) Second, in terms of advertisement and device discovery, Apple’s services and hardware have access to the communication protocols BLE, NFC, and [P2P Wi-Fi (e.g., AWDL)]. For instance, AirDrop discovers nearby AirDrop-capable devices using BLE and AWDL, Apple’s proprietary P2P Wi-Fi communication protocol,⁴⁰⁹ as well as NFC using Apple’s “Tap to Share” feature for NFC-enabled devices.⁴¹⁰

⁴⁰⁴ See <https://developer.apple.com/design/human-interface-guidelines/activity-views>, accessed on 16 September 2024: “App developers can integrate their iOS application into a share sheet by creating an app extension to integrate custom share and action activities into the iOS Share Sheet.”

⁴⁰⁵ Apple’s reply to RFI 1 of 23 September 2024, question 24.

⁴⁰⁶ See <https://support.apple.com/en-us/119857>, accessed on 6 November 2024; Apple’s submission [...] of 14 November 2024, paragraphs 6 and 13.

⁴⁰⁷ See <https://support.apple.com/en-us/119857>, accessed on 16 September 2024.

⁴⁰⁸ Apple’s internal document [...].

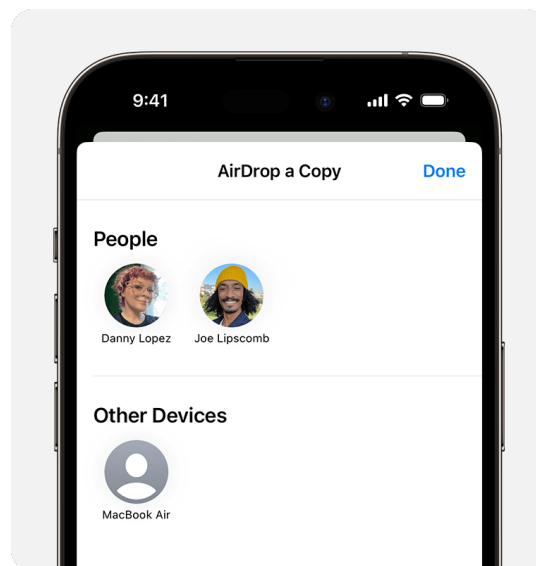
⁴⁰⁹ Apple’s reply to RFI 1 of 23 September 2024, question 19; Apple’s reply to RFI 3 of 7 October 2024, introduction (page 2) and question 17.

⁴¹⁰ See <https://support.apple.com/en-us/119857>, accessed on 16 September 2024; Apple’s internal document [...].

For instance, newer iOS devices support NameDrop, a feature of AirDrop where nearby unlocked iPhones or Apple Watches discover each other using NFC by bringing these devices together. The purpose of NameDrop is to exchange contact information between iPhones and/or Apple Watches.⁴¹¹

- (373) *Third*, Apple uses a device discovery protocol that is intended to enable private and secure discovery between trusted devices before enabling an AirDrop file transfer. The device discovery protocol can filter incoming AirDrop requests based on whether the shared file is being sent from an Apple device that is trusted, i.e. associated with a contact in the destination device's contacts (i.e. Contacts Only mode) or owned by the device's user, without additional user prompts to establish trust.⁴¹² End users are able to configure the discoverability of their device in iOS settings.⁴¹³ Consequently, the end user of the sending device can select their desired destination device from the list of destination devices presented (see Figure 16). This list is shown using *DeviceDiscoveryUI*, a framework that is currently only available to Apple on iOS.⁴¹⁴
- (374) [...] ⁴¹⁵ [...] ⁴¹⁶ [...] ⁴¹⁷

Figure 16: User interface to select a destination device for an AirDrop file transfer on a sending iOS device



Source: <https://support.apple.com/en-us/119857>, accessed on 6 November 2024.

- (375) *Fourth*, in terms of protocols, iOS devices are capable of using several communication protocols, including, but not limited to, infrastructure Wi-Fi, cellular network, Bluetooth, and P2P Wi-Fi communication protocols such as Wi-Fi Aware

⁴¹¹ Apple's internal document [...]; Apple's reply to RFI 1 of 23 September 2024, question 22; Technical meeting Apple/Commission of 3 October 2024, slide deck page 17.

⁴¹² See <https://support.apple.com/en-us/119857>, accessed on 6 November 2024. The Commission understands that, in particular, other devices owned by the user are automatically trusted through "iCloud AutoPair." See Apple's internal document [...].

⁴¹³ See <https://support.apple.com/en-us/119857>, accessed on 6 November 2024.

⁴¹⁴ Technical meeting Apple/Commission of 14 October 2024, slide deck page 6.

⁴¹⁵ Apple's reply to RFI 5 of 16 October 2024, introduction to Section 2.2, page 13.

⁴¹⁶ Apple's reply to RFI 5 of 16 October 2024, introduction to Section 2.2, page 13 and reply to question 34.

⁴¹⁷ Apple's reply to RFI 5 of 16 October 2024, introduction to Section 2.2, page 13.

and AWDL.⁴¹⁸ For instance, the AirDrop file sharing protocol that is embedded in the iOS operating system establishes such a connection between two Apple devices for file transfers using BLE and AWDL.⁴¹⁹ Furthermore, iOS is capable of switching the communication protocol when two nearby devices move out of range. For instance, AirDrop can switch to another communication technology (e.g. infrastructure Wi-Fi, cellular network) if it is faster than AWDL or if the devices move out of the AWDL range using the “Continue over Internet” and “Walk Away” features.⁴²⁰

(376) *Fifth*, in terms of background execution, Apple can execute item sharing in the background on iOS devices through a privileged background process (“daemon”⁴²¹) that is only available to Apple’s services and hardware.⁴²² In particular, this implies that file sharing via AirDrop can be initiated without any further end user action.

(377) *Last*, in terms of file context, iOS devices have awareness about the associated iOS app from which a file was shared. After the file has been sent via AirDrop from an iOS device, the receiving device will save the file(s) on the device. Usually, the files transferred via AirDrop will appear on the same app in the receiving device as they were sent from by the sending device, the Apple Files app, or other system apps (e.g. contacts in the Contacts app, photos in the Photos app, voice memos in the Voice Memo app, boarding passes in the Wallet app).⁴²³

5.7.4. *Current implementation for third-party services and hardware*

(378) Apple makes certain functionalities available to third parties with respect to close-range file transfer between an iOS device and a third-party connected physical device, provided that an end user has downloaded the third-party iOS app that enables close-range file transfers.

(379) In particular, Apple provides a number of frameworks to third-party iOS developers, that enable device discovery, whereby the *MultipeerConnectivity* framework can be used to discover nearby Apple devices, and the *Network* framework can be used to discover both Apple and third-party devices.⁴²⁴ Similarly, third parties can use these two frameworks to establish a P2P Wi-Fi connection between Apple devices using AWDL, but not between Apple and third-party devices.

(380) Furthermore, third-party app developers can make files transferrable to other Apple devices via AirDrop by adding sharing capabilities into their apps, which is done by

⁴¹⁸ Apple’s reply to RFI 5 of 16 October 2024, introduction to Section 2.2, page 13 and reply to question 34.

⁴¹⁹ Apple’s reply to RFI 3 of 7 October 2024, question 17; Technical meeting Apple/Commission of 14 October 2024, AirDrop slide deck page 3.

⁴²⁰ Technical meeting Apple/Commission of 3 October 2024, slide deck page 17; Apple’s reply to RFI 1 of 23 September 2024, question 19; Apple’s reply to RFI 3 of 7 October 2024, question 23; Apple’s internal document [...].

⁴²¹ See recitals (307)-(309) of this Decision on iOS daemons.

⁴²² The Commission understands that AirDrop file sharing is supported by the *sharingd* daemon, an iOS process which allows to execute actions in the background (Section 5.6.3 of this Decision). See Stute et al., “A Billion Open Interfaces for Eve and Mallory: MitM, DoS, and Tracking Attacks on iOS and macOS Through Apple Wireless Direct Link,” 28th USENIX Security Symposium, 2019, <https://www.usenix.org/system/files/sec19-stute.pdf>, accessed on 6 November 2024.

⁴²³ See <https://support.apple.com/en-us/119857>, accessed on 16 September 2024.

⁴²⁴ Apple’s reply to RFI 5 of 16 October 2024, question 37.

integrating the iOS Share Sheet into the iOS app using the *UIActivityViewController* or *ShareLink* public APIs.⁴²⁵

(381) However, these functionalities are not the same as are available to Apple's services and hardware. This includes, but is not limited to, the following shortcomings.

- (a) Accessibility. Although third-party apps can be integrated into the iOS Share Sheet, they are typically not displayed as prominently on the Share Sheet as other Apple services and hardware, such as AirDrop. Depending on the communication protocol selected, third-party apps are also required to display additional end user prompts to establish a connection for file sharing (see Section 5.4.4 of this Decision). Furthermore, third-party iOS apps cannot facilitate accessibility on the receiving device in the same manner as AirDrop, which can seamlessly display a system user interface to accept or decline a transfer. Lastly, unlike Apple solutions such as AirDrop, third-party apps do not come pre-installed on an iOS device, which adds significant friction to the user experience. Instead, the receiving device must already have the close-range file transfer solution installed in order to receive a file using a third-party solution.⁴²⁶
- (b) Advertisement and device discovery. Third parties have access to *MultipeerConnectivity*, *Network* and *Core Bluetooth* frameworks to discover both Apple and third-party devices.⁴²⁷ However, third-party iOS apps must already be installed on the receiving device in order to be able to listen and detect advertisements intended for their app, including from the corresponding app on the sending device.⁴²⁸ By contrast, AirDrop is pre-installed on iOS devices, and can therefore discover nearby AirDrop-capable devices without the end user having to actively install AirDrop.
- (c) [...] ⁴²⁹ [...] ⁴³⁰
- (d) Trusted devices. Third-party iOS apps cannot limit the discovery of devices to trusted devices, such as only contacts, in an equivalent way as Apple can for its iOS features, such as AirDrop. [...] Furthermore, a third-party iOS app is, to the best of the Commission's knowledge, not able to automatically consider the end user's own devices as trusted devices as currently available to Apple's services and hardware.
- (e) Pairing can both establish trust between devices or be facilitated through previously established trust. The Commission takes note that Apple plans to allow third-party developers to trust devices by triggering secure PIN pairing with nearby devices through Wi-Fi Aware pairing mode or skip the pairing if trust had already been established.⁴³¹

⁴²⁵ See <https://developer.apple.com/design/human-interface-guidelines/activity-views>, accessed on 16 September 2024; Apple's reply to RFI 6 of 23 October 2024, question 61; Apple's internal document [...].

⁴²⁶ See <https://support.apple.com/en-us/119857>, last accessed on 6 November 2024.

⁴²⁷ Apple's reply to RFI 5 of 16 October 2024, question 37.

⁴²⁸ Apple's submission [...] of 14 November 2024, paragraphs 8 and 13.

⁴²⁹ Apple's reply to RFI 5 of 16 October 2024, questions 37 and 40; Apple's submission [...] of 14 November 2024, paragraph 2.

⁴³⁰ Apple's reply to RFI 5 of 16 October 2024, question 35.

⁴³¹ Apple's submission [...].

- (f) Protocols. Although third-party iOS app developers can establish a P2P Wi-Fi connection between Apple devices using the available connectivity frameworks (*MultipeerConnectivity* and *Network*), the same does not apply for connections between Apple devices and third-party connected physical devices (see recital (186) of this Decision). To the best of the Commission's knowledge, third-party iOS apps are also not capable of seamlessly changing the communication protocol in the same way that Apple's services and hardware, such as AirDrop, are capable of, due to a lack of information and configurability for communication protocols.⁴³²
- (g) [...] ⁴³³ [...] ⁴³⁴
- (h) Background execution. Depending on the communication protocol selected, third-party apps are required to display additional end user prompts to establish a connection for file sharing (see Section 5.4.4 of this Decision), meaning that third-party iOS apps cannot establish a file sharing connection in the background as is available to Apple's services and hardware, including via AirDrop.⁴³⁵ Similarly, third-party iOS apps cannot continue file sharing in the background.⁴³⁶
- (i) File context. Third-party app developers are currently unable to store and show received files in the respective iOS app corresponding to the app from which it was sent. Instead, files are currently only stored in iOS-managed central file storage.⁴³⁷
- (j) The Commission takes note that Apple has indicated that access to *DeviceDiscoveryUI* would provide third-party app developers with access to features such as enabling extensive app-to-app communication between Apple devices.⁴³⁸
- (382) Therefore, the Commission considers that there is currently an interoperability gap when it comes to third-party connected physical devices connected to iOS devices and that it should specify how Apple has to fill this gap to comply with Article 6(7) of Regulation (EU) 2022/1925.

5.7.5. *The gatekeeper's view*

- (383) While Apples does not appear to contest that it needs to provide some form of interoperability with the close-range wireless file transfer features, Apple raises certain objections as to the scope and feasibility of the measures detailed in the Preliminary Findings.
- (384) *First*, Apple submits that two measures envisaged by the Commission go beyond what is necessary to provide third parties with effective interoperability in relation to close-range wireless file transfer features. The two measures relate to the ability of third-party close-range wireless file transfer solutions (i) to guide the end user of a

⁴³² [Third-party developer]'s reply to RFI 1 of [Confidential], Table 1.

⁴³³ Technical meeting Apple/Commission of 14 October 2024, AirDrop slide deck page 3.

⁴³⁴ Apple's submission [...].

⁴³⁵ [Third-party developer]'s reply to RFI 1 of [Confidential], question 7.

⁴³⁶ [Third-party developer]'s reply to RFI 1 of [Confidential], questions 7 and 8; Agreed minutes of meeting with [third-party developer] of 24 October 2024, paragraph 7.

⁴³⁷ [Third-party developer]'s submission of 15 October 2024, page 1.

⁴³⁸ Technical meeting Apple/Commission of 14 October 2024, AirDrop slide deck page 3.

receiving device to the relevant app store and (ii) to indicate that a file has been shared via a specific app. Apple argues that these functionalities are not used by or available to Apple's AirDrop and are therefore not required to be made available to third parties under Article 6(7) of Regulation (EU) 1925/2022.

(385) *Second*, with regard to the ability to guide end users to the relevant app store if the close-range wireless file transfer solution is not installed on the receiving device (point (i)), Apple submits that the ability raises security and privacy risks that cannot otherwise be mitigated.⁴³⁹ [...] ⁴⁴⁰

(386) [...] ⁴⁴¹ [...]

(387) [...] ⁴⁴² In particular, the technical solution envisaged for the latter measure would allow third-party apps to contribute the user's identity and contacts.

(388) [...] ⁴⁴³ *First*, some interoperability solutions will depend on whether NFC is included in Wi-Fi Aware 5.0. ⁴⁴⁴ [...] ⁴⁴⁵ [...] ⁴⁴⁶

5.7.6. *The Commission's assessment*

(389) The Commission considers that Apple can and should provide interoperability to the features of close-range wireless file transfer solutions as described in Section 5.7.1 of this Decision, subject to certain modifications in reply to Apple's comments.

(390) *First*, guiding the end user of a receiving device to the relevant app store to facilitate the installation of a close-range wireless file transfer solution is necessary to provide effective interoperability. As explained in Section 3.1.1 of this Decision, the Commission considers that Article 6(7) of Regulation (EU) 2022/1925 does not require the Commission to demonstrate that each of the measures is individually necessary to enable contestability, i.e. that (some) third parties are able to provide a "*competitive offering*" or an "*alternative solution*," which is enough for achieving contestability. Such assessment would reintroduce the requirement to investigate on a case-by-case basis the effects on competition of a gatekeeper's given conduct, which the legislator explicitly rejected and which is contrary to the text and purpose of Article 6(7) of Regulation (EU) 2022/1925. Under the correct legal test, the measure is necessary to reduce the gap between the conditions under which Apple and third parties operate.

(391) In particular, the Commission considers that without the measures in the Annex to this Decision, third-party providers of close-range wireless file transfer solutions will always be at a significant disadvantage compared to Apple: the installation of a close-range wireless file transfer app involves higher user friction compared to using AirDrop, which is pre-installed on iOS devices, and which makes it more challenging for third parties to counter the network effects enabled by the pre-installation of AirDrop.

⁴³⁹ Apple's reply to the Preliminary Findings, paragraph 228.

⁴⁴⁰ Apple's submission of 29 January 2025, page 2.

⁴⁴¹ Email from Apple to the Commission on 13 February 2025 [on the draft final measures].

⁴⁴² Email from Apple to the Commission on 13 February 2025 [on the draft final measures].

⁴⁴³ Apple's reply to the Preliminary Findings, paragraph 223.

⁴⁴⁴ Apple's reply to the Preliminary Findings, paragraph 231.

⁴⁴⁵ Apple's reply to the Preliminary Findings, paragraph 224, fifth subpoint.

⁴⁴⁶ Email from Apple to the Commission of 3 February 2025 [on the draft final measures].

- (392) *Second*, contrary to Apple security and privacy concerns regarding the guiding of an end user to install a close-range wireless file transfer solution, and as set out in Section 3.3 of this Decision, the gatekeeper must demonstrate, using data or other means, the existence and magnitude of the integrity risk before defining an integrity measure. However, the security and privacy concerns Apple put on the table are neither integrity concerns, nor of a concrete nature. [...] In addition, and in line with Apple's arguments that devices must be paired for technical feasibility, the Commission has limited the measure to paired devices in the Annex to this Decision.
- (393) Furthermore, the Commission has reformulated the measures related to trusted devices to encompass the measures that make use of the same technical solution into one measure. [...] ⁴⁴⁷ Similarly, and without prejudice as to whether the Commission considers the measure indicating that a file has been shared via a specific app to be within the scope of Article 6(7) of Regulation (EU) 2022/1925 or not, the Commission has not included that measure in this Decision.
- (394) *Third*, as regards timing, Apple's two-step approach appears acceptable. This means that Apple would need to (i) enable the scenario of close-range wireless file transfers while the receiving device has the relevant app open by spring 2026, and (ii) implement all measures for the features of close-range wireless file transfer solutions by fall 2026.
- (395) However, the Commission does not agree with Apple's conditionality on the inclusion of NFC into the Wi-Fi Aware 5.0 specification. The Commission considers that Apple should make all measures for the features of close-range wireless file transfer solutions available to third parties by fall 2026, regardless of whether the solution is based on Wi-Fi Aware 5.0 or not. *First*, Apple's current AirDrop implementation (e.g. NameDrop) demonstrates Apple's ability to pair devices via NFC without using Wi-Fi Aware. *Second*, as Apple has explained extensively in its response to the Preliminary Findings with regards to the P2P Wi-Fi connection feature, Apple does not control the development of the Wi-Fi Aware standard in the Wi-Fi Alliance. ⁴⁴⁸ Apple's interoperability solution to provide equal conditions to third parties for the features of close-range wireless file transfers cannot be bounded by the developments of the Wi-Fi Aware standard. Apple should therefore provide, if needed, an NFC-based solution that is independent of Wi-Fi Aware.

5.7.7. *Measures that Apple should implement*

- (396) To meet the requirements of Article 6(7) of Regulation (EU) 2022/1925, Apple should implement an interoperability solution that provides third parties with access to the same features for close-range wireless file transfer solutions as available to Apple (as described in Section 5.7.1 of this Decision), in a way that is equally effective as the solution available to Apple. For the avoidance of doubt, this includes file sharing between an iOS device and a nearby Apple or third-party connected physical device.
- (397) Apple should allow third parties effective interoperability with the same features for close-range wireless file transfer solutions controlled by iOS and their functionalities as available to Apple's own connected physical devices (including via AirDrop ⁴⁴⁹),

⁴⁴⁷ Email from Apple to the Commission on 13 February 2025 [on the draft final measures].

⁴⁴⁸ Apple's reply to the Preliminary Findings, paragraphs 200-201.

⁴⁴⁹ As well as Apple's alternatives or successors to AirDrop.

including, but not limited to, Apple Watch, Apple Vision Pro, as well as any future Apple connected physical devices. Apple should implement an interoperability solution that is equally effective as the solution available to Apple. To that end, Apple should make the following features available to third-party close-range wireless file transfer solutions as described in recital (365) of this Decision.

- (398) To provide third parties with an interoperability solution for iOS features of close-range wireless file transfer solutions that is equally effective as that available to any of Apple's own connected physical devices, Apple should implement the following measures.

(a) Accessibility

- (1) Apple should allow close-range wireless file transfer solutions to be displayed via the same user interface (e.g. iOS Share Sheet) and under the same conditions as Apple's wireless file transfer services, such as AirDrop, are displayed.⁴⁵⁰
- (2) Apple should allow third-party close-range file transfer solutions to launch a close-range wireless file transfer by tapping on the respective service in the relevant iOS user interface as available to Apple (e.g. iOS Share Sheet), which ultimately allows the end user to use the solution without the need to open the third-party solution into the foreground.
- (3) Apple should allow third-party close-range wireless file transfer solutions to trigger the system user interface responsible for the file transfer on the sending or receiving iOS device, provided that the receiving device has the solution installed.⁴⁵¹ This may include a user experience to trigger device pairing or a notification to launch and connect a close-range wireless file transfer solution. The user experience for the end user using a third-party solution should be under equal conditions as when using an Apple solution such as AirDrop, both on the sending and the receiving device.
- (4) In the event that the close-range wireless file transfer solution is not installed on the receiving device, Apple should allow the sending device to discover the paired receiving device, and should allow the user of the receiving device to be informed of an incoming file (e.g. via a notification, app clip, system user interface) and to be guided to the appropriate app store in order to facilitate the installation of the close-range wireless file transfer solution.⁴⁵²

⁴⁵⁰ As set out in recital (81), an interoperability solution should not impose undue costs for other third parties that are involved in the use of the relevant feature (here, providers of apps that implement the iOS Share Sheet), as this would ultimately affect the effectiveness of the solution for the third parties that are beneficiaries of the solution (here, providers of file transfer solutions).

⁴⁵¹ See the AirDrop user interface on the receiving iOS device in Figure 15 of this Decision for reference. The sender iOS device also shows or updates a system user interface that indicates, for instance, when the file transfer has been completed.

⁴⁵² As set out in recital (391) of this Decision, the Commission considers that third-party close-range wireless file transfer solutions are at a significant disadvantage compared to Apple in terms of end-to-end user experience: whereas AirDrop is pre-installed on iOS devices, third-party solutions have to first be installed by the end user. This measure therefore aims to ensure that third parties can offer close-range wireless file transfer solutions with an end-to-end user experience for sending a file, regardless of whether the third-party solution is installed on the receiving device.

- (5) Apple should allow the end user to set the same options and preferences in settings for third-party close-range file transfer solutions, including selecting between “Everyone” and “Contacts only” and adjusting the time limitations of the Everyone Mode, as are available to Apple. Apple should treat these settings in the same way as it treats settings for its own close-range wireless file transfer solutions, such as AirDrop.⁴⁵³
- (b) Advertisement and device discovery
 - (1) Apple should allow close-range wireless file transfer solutions to discover nearby Apple and non-Apple connected physical devices using protocols that include, but are not limited to, BLE, a P2P Wi-Fi connection, and NFC.
 - (2) Apple should allow third-party connected physical devices to discover nearby iOS devices for close-range wireless file transfers using protocols that include, but are not limited to, BLE, a P2P Wi-Fi connection, and NFC.
 - (3) Apple should allow close-range wireless file transfer solutions access to the iOS functionality that scans for advertisements for close-range wireless file transfers from nearby connected physical devices under equal conditions as is available to Apple’s own close-range wireless file transfer solutions, such as AirDrop (e.g. that both devices have their screen on).
 - (c) Trusted devices
 - (1) Apple should allow close-range wireless file transfer solutions to trust a device via the operating system, such that future file transfers do not require re-establishing this trust. Subject to revokable end user consent, the device should remain trusted. Furthermore, the process for third-party solutions to trust another device should be subject to equal conditions as available to Apple’s solutions, such as AirDrop, including the user experience for trusting devices that belong to the same end user or trusting devices from the end user’s contacts.⁴⁵⁴
 - (2) Apple should allow close-range wireless file transfer solutions to limit device discovery of nearby connected physical devices to devices that the end user has previously trusted, regardless of whether the trusted device is an Apple or third-party device, based on the user’s choice for the device discovery mode.
 - (d) Protocols
 - (1) Apple should allow close-range wireless file transfer solutions to use any communication protocol available to Apple’s services or hardware, which includes but is not limited to, BLE, infrastructure Wi-Fi, cellular network and P2P Wi-Fi connection, to transfer files between the iOS device and nearby Apple or third-party connected physical devices (and vice-versa).

⁴⁵³ For instance, AirDrop settings must not override the settings for third-party close-range wireless file transfer iOS apps, unless settings for the latter would equally override settings for AirDrop.

⁴⁵⁴ Apple’s submission [...].

- (2) Apple should allow close-range wireless file transfer solutions to integrate their own file transfer protocols based on communication protocols.
 - (3) Apple should allow close-range wireless file transfer solutions to change the communication protocol, for instance in the case where a faster alternative communication channel is available, and providing third-party solutions with the relevant information in order to make such a decision.
 - (4) Apple should allow close-range wireless file transfer solutions to continue file sharing if the devices involved in the file transfer move out of wireless range using any other available connection (e.g. infrastructure Wi-Fi, cellular network), and provide the relevant connection metadata to indicate that the devices moved out of wireless range.
- (e) Background execution
- (1) Apple should allow close-range wireless file transfer solutions with the same background execution abilities as are available to Apple's solutions, such as AirDrop. This includes, but is not limited to, the ability to launch the file sharing protocol without needing to open the close-range wireless file transfer solution (e.g. via the iOS Share Sheet as explained in Section 5.7.3 of this Decision) to send or receive files.
 - (2) Apple should allow close-range wireless file transfer solutions to continue receiving and sending files that are being transferred in the background after the transfer started, meaning that the app in which the file transfer was initiated does not need to remain in the foreground. Apple may require that the progress of the file transfer is presented to the user while it is ongoing and the iPhone screen is on, as long as Apple's solutions, such as AirDrop, are subject to the same requirement and the close-range wireless file transfer solution can do so through an equivalent interface to Apple's solutions.
- (f) File context. Apple should allow close-range wireless file transfer solutions to open and store the receiving file under equal conditions as Apple's solutions, such as AirDrop, are capable of opening and storing a receiving file. This could, for instance, include sharing relevant metadata alongside the file that is also available to Apple's connected physical devices, or prompting an end user to open the received file in a specific app.
- (399) Apple should grant third parties access to additional functionalities if necessary to enable effective interoperability with the features for close-range wireless file transfer solutions described in Section 5.7.1 of this Decision.
- (400) Apple should also provide effective interoperability with any future updates, including new functionalities, of the iOS features used for close-range wireless file transfer solutions insofar as they are available to Apple's own connected physical devices. To this end, the general measures in Section 5.12 of this Decision apply, including in particular the measures concerning future updates and new functionalities set out in Section 5.12.7 in this Decision.
- (401) Apple should implement the measures above in compliance with the measures for all features in Section 5.12 of this Decision.

5.7.8. *Implementation timing*

- (402) Apple should implement the measures required to enable the scenario of close-range wireless file transfers while the receiving device has the relevant close-range wireless file transfer solution open by 1 June 2026. Apple should implement all measures for the features for close-range wireless file transfer solutions in the release of iOS 20, and in any case by the end of 2026.

5.8. **Measures for automatic Wi-Fi connection**

- (403) iPhone users may connect to Wi-Fi networks in several ways, including by manually selecting the network and entering the password. After doing so, the Wi-Fi network credentials are saved on the iPhone, so that the iPhone can automatically reconnect to the network whenever it is within range again. Apple connected physical devices can access these credentials saved on the iPhone and automatically connect to the corresponding networks, without the user having to manually add each of them on each connected physical device. This functionality is made possible by Apple's privileged interoperability with relevant iOS features.
- (404) Third-party connected physical devices are not able to use the same iOS feature, even with the end user's permission. Users must instead manually select and re-enter the password for every Wi-Fi network they want the connected physical device to connect to, which may be particularly cumbersome on devices with small screens. As a result, end users of third-party connected physical devices do not enjoy the same frictionless experience, which reduces the attractiveness of such devices compared to Apple devices.

5.8.1. *Description of the feature*

- (405) The automatic Wi-Fi connection feature consists in the access of connected physical devices to information about local infrastructure Wi-Fi networks saved on the iPhone, to allow connected physical devices to join these networks without additional end user engagement.
- (406) Some connected physical devices are able to directly connect to a local infrastructure Wi-Fi connection to access the internet. This is the case for more sophisticated devices such as smartwatches, virtual and augmented reality glasses, or tablets. To establish a local Wi-Fi connection, the device must scan for available Wi-Fi networks and the end user must select a network and enter the correct password. End users often use multiple Wi-Fi networks, for instance at home, at the workplace, and at the homes of friends and family. This means that end users must complete the process of entering credentials for each Wi-Fi network they intend to connect the connected physical device to.
- (407) Identifying the correct Wi-Fi network, obtaining the credentials, and entering the credentials for each new connected physical device can be an onerous process. The form factor of the connected physical device may further complicate this process. For instance, a smartwatch will typically have a small screen, which makes it difficult and time-consuming to enter a Wi-Fi password, which can be long and complex. Some connected physical devices do not have an interface suitable to enter Wi-Fi credentials, meaning the password must be entered in the companion app on the connected iOS device instead.
- (408) iOS devices save certain information for each Wi-Fi network that the end user connected to in the past ("Wi-Fi Network Information"). According to Apple, this includes the following information: SSID (network name), BSSID (access point

identifier), indication if the SSID is broadcasted or not, indication if Private Relay is enabled or not, and security configurations being the password and 802.11 WPA or RSN information elements.⁴⁵⁵

- (409) iOS devices can use the Wi-Fi Network Information to automatically reconnect to previously visited Wi-Fi networks when in range. In addition, the Wi-Fi Network Information can be transmitted to Apple's connected physical devices, which can use this information to automatically connect to Wi-Fi networks without additional end user engagement.

5.8.2. Feature falls within the scope of Article 6(7) of Regulation (EU) 2022/1925

- (410) The Commission finds that the automatic Wi-Fi connection feature as described in Section 5.8.1 of this Decision falls within the scope of Article 6(7) of Regulation (EU) 2022/1925. Automatic Wi-Fi connection is a feature which is controlled via iOS, Apple's operating systems for iPhones, which is listed in the Designation Decision.

5.8.3. Current implementation for Apple's own services and hardware

- (411) Apple uses the automatic Wi-Fi connection feature to seamlessly synchronise saved Wi-Fi networks between iOS devices and Apple connected physical devices. In particular, iOS devices transmit Wi-Fi Network Information to the Apple Watch, the Apple Vision Pro, and other Apple connected physical devices which are associated with, and logged into, the same Apple Account as the iOS device upon pairing the Apple connected physical device with the iOS device.
- (412) After being paired, the Apple connected physical device will continue to receive updated Wi-Fi Network Information, reflecting new additional Wi-Fi networks that the end user connects to on the iOS device, or Wi-Fi networks that the user chooses to forget.⁴⁵⁶
- (413) Apple's connected physical devices use the Wi-Fi Network Information to automatically connect with nearby local Wi-Fi networks, i.e. without the need for the end user to select the Wi-Fi network or enter credentials. Neither the iOS device nor the Apple connected physical device request consent from the end user before transmitting or using the Wi-Fi Network Information.⁴⁵⁷
- (414) The iOS device also transmits Wi-Fi Network Information to Apple connected physical devices for Wi-Fi networks to which the iOS device connected prior to pairing the Apple connected physical device (historical Wi-Fi data). The Apple connected physical device can thus connect to these Wi-Fi networks independently of the iOS device. For instance, the iOS device may be elsewhere or powered off.

5.8.4. Current implementation for third-party services and hardware

- (415) Apple does not currently transmit or otherwise share Wi-Fi Network Information with third-party developers or third-party connected physical devices.⁴⁵⁸ As a result,

⁴⁵⁵ Apple's reply to RFI 6 of 23 October 2024, question 12.

⁴⁵⁶ Apple's reply to RFI 4 of 14 October 2024, question 31; Apple's reply to RFI 6 of 23 October 2024, question 12.

⁴⁵⁷ Alternatively, Apple Watch users can also enter the password manually on the Apple Watch, if they so choose. See <https://support.apple.com/en-us/111818>, accessed on 17 November 2024.

⁴⁵⁸ Apple's reply to RFI 4 of 14 October 2024, question 31; Apple's reply to RFI 6 of 23 October 2024, question 12.

third-party connected physical devices are currently not able to automatically connect to Wi-Fi networks for which the end user's iOS device has saved Wi-Fi Network Information. Instead, a third-party connected physical device must first scan for all available Wi-Fi networks, which is an energy-consuming task,⁴⁵⁹ and the end user must then select a Wi-Fi network from a list of available Wi-Fi networks and enter the credentials. This process must be repeated for each Wi-Fi network that the end user wants to connect to.

- (416) Therefore, the Commission considers that there is currently an interoperability gap when it comes to third-party connected physical devices connected to iOS devices and that it should specify how Apple has to fill this gap to comply with Article 6(7) of Regulation (EU) 2022/1925.

5.8.5. *The gatekeeper's view*

- (417) *First*, Apple argues that access to the automatic Wi-Fi connection feature goes beyond what is needed to ensure effective interoperability, as third-party connected physical devices can establish Wi-Fi connections without making use of the feature. According to Apple, the feature is simply an easier way of establishing a Wi-Fi connection. Apple also argues that there is no indication of interested or concerned third parties.⁴⁶⁰
- (418) *Second*, Apple submits that the feature should be limited to the Wi-Fi Network Information that Apple shares with its own connected physical devices and limited to the Wi-Fi networks for which the iOS device shares Wi-Fi Network Information with its own connected physical devices.⁴⁶¹
- (419) *Third*, Apple submits that the automatic Wi-Fi connection feature jeopardises integrity and security of user networks and connected physical devices and raises significant privacy concerns. Apple claims that Wi-Fi Network Information reveal sensitive information, such as the names of sensitive locations (e.g. doctor's offices), user's medical devices, user's home and work networks, and businesses that users frequent. According to Apple, malicious actors could use this information to identify and fingerprint users or monitor a user's presence and absence. They could also upload a user's networks and passwords to insecure servers or allow third-party devices to access restricted networks the user has access to (e.g. a work network, a hospital network). Apple submits that it cannot ensure safe handling of Wi-Fi network information by third parties because Apple does not control third-party software or devices. By contrast, sharing Wi-Fi Network Information among Apple devices is acceptable because the user is signed in with the same Apple Account into these devices. Such an Apple Account does not exist in case of a third-party device.⁴⁶²
- (420) *Fourth*, notwithstanding Apple's view that it is not required to provide interoperability with the automatic Wi-Fi connection feature, [...].⁴⁶³ [...] ⁴⁶⁴ [...] ⁴⁶⁵

⁴⁵⁹ Choi et al. "Energy-efficient WiFi scanning for localization," *Pervasive and Mobile Computing* 37 (2017) 124-138, DOI 10.1016/j.pmcj.2016.07.005.

⁴⁶⁰ Apple's reply to the Preliminary Findings, paragraphs 331-332.

⁴⁶¹ Apple's mark-up of the Commission's proposed measures of 23 January, paragraphs 111-120; Agreed minutes of meeting on 11 and 12 February 2025.

⁴⁶² Apple's reply to the Preliminary Findings, paragraphs 336-343, 24-26, 86.

⁴⁶³ Apple's reply to the Preliminary Findings, paragraph 344.

⁴⁶⁴ Email from Apple to the Commission of 3 February 2025.

5.8.6. *The Commission's assessment*

- (421) Apple's position that interoperability with the automatic Wi-Fi connection feature is not required as third parties are already able to establish Wi-Fi connections without it cannot be accepted. The relevant feature is not establishing a Wi-Fi connection, it is to share Wi-Fi Network Information. That it is possible for end users to connect a third-party connected physical device to a Wi-Fi network without access to the feature – in a burdensome way – does not release Apple from its obligation to allow effective interoperability. Apple implemented the feature for Apple connected physical devices precisely to relieve end users of this burden (see also Section 3.1.1 of this Decision).
- (422) As concerns the claim that there are no interested or concerned third parties for this feature, the Commission considers that this is not determinative for Apple's obligation to allow interoperability (see recital (17) of this Decision). In any event, the claim is also incorrect. Apple received a request for this feature in its Interoperability Request Portal as early as 9 March 2024.⁴⁶⁶ The fact that Apple offers this feature to users of its own connected physical devices underlines its relevance.
- (423) The Commission clarifies in the measures in the Annex to this Decision that the feature is limited to the Wi-Fi Network Information that Apple shares with its own connected physical devices and limited to the Wi-Fi networks for which the iOS device shares Wi-Fi Network Information with its own connected physical devices.

5.8.6.1. Concerning integrity

- (424) [...] ⁴⁶⁷ [...] [Third-party developer] submitted that effective interoperability requires a one-time prompt (i.e. not on a per-network basis) and the inclusion of historic Wi-Fi network information.⁴⁶⁸
- (425) The Commission notes the following regarding Apple's justification.
- (426) *First*, Apple does not raise integrity concerns regarding the feasibility of building an interoperability solution, i.e. that Apple cannot technically implement the feature. Any alleged integrity issue would thus be limited to the implementation phase, i.e. the adjustments under which that solution is made available to third parties.⁴⁶⁹
- (427) *Second*, as outlined in Section 3.3 of this Decision, the burden is on Apple to duly justify the measures it intends to take to mitigate integrity risks as necessary and proportionate in the context of implementing the effective interoperability. Apple has not substantiated that the alleged risks could compromise the integrity of iOS or of the automatic Wi-Fi connection feature. It appears that neither the functioning of iOS nor the Wi-Fi connection would be impaired.
- (428) Apple's concerns about third-party access to data that could be sensitive to the user appears to be a privacy concern. As explained in Section 3.3 of this Decision, the legislator intentionally did not allow for a justification based on privacy grounds and compliance with the service providers' specific obligations in the areas of data

⁴⁶⁵ Email from Apple to the Commission of 17 February 2025 [on the draft final measures].

⁴⁶⁶ One request submitted by [third-party developer] on 9 March 2024 through the Interoperability Request Portal.

⁴⁶⁷ See Apple's mark-up of the Commission's proposed measures of 23 January.

⁴⁶⁸ [Third-party developer]'s submission of 29 January 2025 paragraphs 7.3.3-7.3.5.

⁴⁶⁹ Agreed minutes of meetings with Apple on 11 and 12 February 2025.

protection falls within the competence of the public authorities in charge of those respective sectors. In particular, both Apple and the providers of services or hardware requesting effective interoperability under Article 6(7) of Regulation (EU) 2022/1925 are subject to Regulation (EU) 2016/679 (GDPR). Privacy and security elements can be relevant to ensure that Article 6(7) of Regulation (EU) 2022/1925 is applied in conformity with fundamental rights, taking due consideration that the Union legislator limited the justification to integrity having weighed the public interests against the private interests of economic operators impacted by that legislation.

- (429) *Third*, and in any event, regardless of whether such a privacy concern poses a risk to integrity, such a concern could be addressed by seeking consent from the end user to share the data with third-party connected physical devices. A one-time prompt would create less user friction than a prompt for each Wi-Fi network. Such a measure would be less restrictive of the goal to achieve effective interoperability than not sharing such data with third parties. To achieve a level playing field as intended by Article 6(7) of Regulation (EU) 2022/1925, setting equivalent standards for Apple and third-party devices, such a prompt should also be shown to Apple's own connected physical devices such as the Apple Watch.⁴⁷⁰ Privacy risks may only be proportionately addressed by user prompts applied in a non-discriminatory manner to both Apple and third-party connected physical devices.
- (430) A refusal to share historic Wi-Fi Network Information despite end user consent may also not genuinely reflect a privacy concern in a systematic and consistent manner. While Wi-Fi Network Information can be sensitive, iOS already gives third parties access to information that is similarly or even more sensitive. For instance, iOS enables access of third-party apps to the user's photo library and list of contacts. Such information can contain more sensitive private information about a user than their Wi-Fi networks. In both cases, iOS gives access to this information subject to a one-time user authorisation prompt, which allows to select and grant access only to specific photos / contacts, or alternatively to give full access to all photos / contacts.
- (431) *Fourth*, Apple argues that it controls what Apple connected physical devices do with Wi-Fi network data, but not what third-party connected physical devices would do, e.g. upload the data to a server. Further, third-party connected physical devices lack the required trust because end users cannot sign into their Apple Account with these devices. As explained in Section 3.3 of this Decision, this condition appears to be exclusively in Apple's control because Apple decides which devices can sign into an Apple Account.

5.8.6.2. Concerning timing

- (432) Apple submits that the implementation timing for automatic Wi-Fi connection proposed in the Preliminary Findings is not feasible, as the Commission did not raise this feature with Apple previously, and Apple therefore was not yet able to make a proposal for an interoperability solution.⁴⁷¹ [...] ⁴⁷² [...] ⁴⁷³
- (433) Apple's claim that it was unaware that feature was within the scope of the present proceedings is incorrect. Apple received a request for this feature in its

⁴⁷⁰ [...]

⁴⁷¹ Apple's reply to the Preliminary Findings, paragraph 344.

⁴⁷² Email from Apple to the Commission of 3 February 2025.

⁴⁷³ [...].

Interoperability Request Portal as early as 9 March 2024.⁴⁷⁴ This was after Article 6(7) of Regulation (EU) 2022/1925 became effective for Apple with regard to iOS on 7 March 2024. The Commission asked Apple questions on this feature from an early stage of the proceedings.⁴⁷⁵ Apple has therefore had a significant amount of time to consider and work on an interoperability solution for automatic Wi-Fi connection.

(434) [...] ⁴⁷⁶ [...] ⁴⁷⁷

5.8.7. *Measures that Apple should implement*

- (435) To meet the requirements of Article 6(7) of Regulation (EU) 2022/1925, Apple should implement an interoperability solution that provides third parties with access to the same automatic Wi-Fi connection feature as available to Apple (as described in Section 5.8.1 of this Decision), in a way that is equally effective as the solution available to Apple.
- (436) Apple should make available to third-party connected physical devices Wi-Fi Network Information saved on the end user's iOS device for Wi-Fi networks for which Apple shares such information with any of its own connected physical devices.
- (437) "Wi-Fi Network Information" consists of the information which the iOS device shares with Apple's own connected physical devices. This may include for each Wi-Fi network: SSID (network name), indication if the SSID is broadcasted or not, the network password (if applicable), and the network security configuration. It may also include BSSID (access point identifier) and the Wi-Fi Channel number.
- (438) Apple should provide third-party iOS companion apps with the Wi-Fi Network Information for transmission to third-party connected physical devices.
- (439) Apple should share the Wi-Fi Network Information at the same cadence as it does for its own connected physical devices.
- (440) Apple may seek permission from the user for sharing "Wi-Fi Network Information" via a permission prompt in compliance with the requirements of Article 6(7) of Regulation (EU) 2022/1925. Among consent options that Apple offers to the user there must be a one-time permission, so that such permission also applies to all Wi-Fi networks to which the iOS device connects in the future (provided the Wi-Fi network is in scope of recital (437)) of this Decision.⁴⁷⁸
- (441) Apple should grant third parties access to additional functionalities if necessary to enable effective interoperability with the automatic Wi-Fi connection feature described in Section 5.8.1 of this Decision.

⁴⁷⁴ One request submitted by [third-party developer] on 9 March 2024 through the Interoperability Request Portal.

⁴⁷⁵ See e.g. Apple's reply to RFI 4 of 14 October 2024, question 31; Apple's reply to RFI 6 of 23 October 2024, question 12.

⁴⁷⁶ Email from Apple to the Commission of 17 February 2025 [on draft final measures].

⁴⁷⁷ Email from Apple to the Commission of 17 February 2025 [on draft final measures].

⁴⁷⁸ This requirement aims to reduce user friction. This measure shall not prevent Apple from showing more granular prompts, or showing prompts at a higher frequency, provided that Apple shows equivalent prompts in terms of granularity and frequency to users of its own connected physical devices. It shall also not prevent Apple from not showing any prompts with respect to third-party connected physical devices. [...]

- (442) Apple should implement the measures above in compliance with the measures for all features in Section 5.12 of this Decision.
- (443) Apple shall also provide effective interoperability with any future updates, including new functionalities, of the automatic Wi-Fi connection feature insofar as they are available to Apple's own connected physical devices. To this end, the general measures in Section 5.12 of this Decision apply, including in particular the measures concerning future updates and new functionalities set out in Section 5.12.7 in this Decision.

5.8.8. Implementation timing

- (444) Apple should implement all measures to provide effective interoperability with the automatic Wi-Fi connection feature in the next major iOS release, i.e. iOS 19, and in any case by the end of 2025 at the latest. By the end of 2025, the solution must provide access to the following Wi-Fi Network Information: SSID (network name), an indication if the SSID is broadcasted or not, the network password (if applicable), and the network security configuration.
- (445) Apple should update the solution to provide access to the Wi-Fi Network Information that Apple shares with any of its own connected physical devices by 1 June 2026 at the latest.

5.9. Measures for media casting

- (446) Apple provides a media casting feature called AirPlay, that is integrated into iOS. From any app that plays media audio and video content, AirPlay is automatically available to cast that content to AirPlay receivers, such as the Apple TV or the Apple Vision Pro, or certified third-party connected physical devices. Additionally, when mirroring an iOS device's screen, AirPlay is also the most readily available casting solution to the end user, having a dedicated button in the iOS Control Centre which the user can access at any time. Under the hood, AirPlay can automatically and seamlessly find available receivers and uses Apple's proprietary protocol AWDL to deliver a high-quality media stream.
- (447) Third-party developers do not have equal access to features relevant for media casting apps as those available to AirPlay. For example, third-party media casting apps face restrictions in terms of available resources, which can lead to worse quality or even crashing of the casting session. Moreover, the developers of media casting apps cannot make their solution available in a centralised way after the user installs them, becoming available to all apps that play media, as AirPlay is. Overall, AirPlay enjoys privileged interoperability with a set of relevant iOS features that enable a better user experience for media casting.

5.9.1. Description of the feature

- (448) Media casting is the ability to cast audio, video, and mirror screens between an iOS device and a connected physical device. Casting can take place either from an iOS device to a connected physical device, or from a connected physical device to an iOS device. Alternatively, the iOS device can be used to initiate casting between a streaming server (e.g. YouTube) and a connected physical device. In this case the iOS device connects to the connected physical device and sets up the stream, but the media stream itself takes place directly between the streaming server and the receiving device. The iOS device may act as a remote control (e.g. volume control, playback speed, etc.).

Figure 17: Streaming video content from the iPhone to a TV via AirPlay, Apple's media casting solution



Source: <https://www.apple.com/airplay/>, accessed on 6 November 2024.

- (449) Third-party services and hardware can use several casting solutions. AirPlay is one such casting solution and is pre-installed on Apple devices. Other third-party casting solutions include Google Cast, Miracast and Matter casting. On iOS, these casting solutions are typically made available as SDKs that app developers integrate in their apps.⁴⁷⁹ It is attractive for app developers to adopt a casting solution that is supported by many devices. Third-party receiving devices may also require certification to support a third-party casting solution. Third-party receiving devices may support multiple casting solutions.
- (450) Depending on the casting solution, third parties connected physical devices may need to complete a certification process to become a receiving device. For instance, this is the case for Apple's AirPlay casting solution. Third-party devices that are AirPlay compatible feature a logo on their packaging and marketing materials indicating "Works with Apple AirPlay."⁴⁸⁰

Figure 18: Logo indicating that third-party device is compatible with AirPlay



Source: <https://www.apple.com/airplay/>, accessed on 6 November 2024.

- (451) Third parties, in particular those who manufacture their own connected physical devices, may also choose to implement a custom casting solution. For example, this casting solution could be attuned to the requirements of their streaming platform or their connected physical devices, such as advanced video codecs or conversely optimised streams suited for smaller screens.
- (452) The features relating to media casting available to Apple are listed below.

⁴⁷⁹ For example, see the documentation for the Google Cast software development kit, <https://developers.google.com/cast/docs/overview>, accessed on 5 November 2024.

⁴⁸⁰ Apple's reply to RFI 1 of 23 September 2024, question 30.

- (a) Accessibility. A casting solution must be able to be accessed conveniently and intuitively from media casting apps or the operating system. For example, Apple offers the *AVRoutePickerView* API⁴⁸¹ for app developers to integrate a picking menu in their apps, from which users can pick the casting target and casting method. iOS Control Centre also includes picking menus, which are currently only accessible to AirPlay.⁴⁸²
- (b) Centralised availability. A casting solution must have access to operating system resources to function effectively. The casting solution must be made available centrally in a manner where media apps that want to use the casting solution can access it. This prevents that each media app needs to integrate code for the casting solution separately, which give rise to a host of problems, such as redundant code taking up storage space and outdated versions in apps that are not frequently updated.⁴⁸³ The casting solution should also be able to save data independently of the media app, including, but not limited to, storing device authentication metadata centrally so that the user can easily cast content from different apps without having to log into the same casting solution separately for each app playing media content.⁴⁸⁴ The casting solution should also be able to directly access media stored in OS-managed storage or in other apps, without the need to duplicate the media before being able to cast it.⁴⁸⁵
- (c) Advertisement and discovery. Receiver devices advertise their casting capabilities to sender devices. Examples of device capabilities include whether a device supports audio, video, or both; network interfaces supported; and hardware capabilities. The sender device listens for advertisements from receiver devices and shows the receiver devices with the right capabilities in an identifiable manner to the end user in selection screens (“picker” or “picking menu”). Discovery can take place via technologies such as BLE or P2P Wi-Fi. Additionally, proximity hardware such as ultrawide band (“UWB”) and NFC can make casting more convenient, by enabling discovery when devices are near each other (e.g. holding the smartphone next to a speaker).
- (d) Communication protocols. After establishing a connection with the receiving device, the sender initiates a media stream. This can take place via various communication protocols, such as P2P Wi-Fi or, if the sending and receiving device are connected to the same local network, via infrastructure Wi-Fi. When using the phone as a sender to initiate casting from a streaming service to the receiving device, the sender sets up the connection while the media stream takes place directly from the server to the receiving device. The available communication protocols and media streaming protocols based on communication protocols may depend on the capabilities of the sending and receiving device.
- (e) Controls. Once the casting session is ongoing, the iPhone can be used to control the media playback. This includes using the hardware buttons to control the volume, as well as on-screen buttons to e.g. pause or fast forward.

⁴⁸¹ See <https://developer.apple.com/documentation/avkit/avroutepickerview>, accessed 18 November 2024.

⁴⁸² Apple’s reply to RFI 4 of 16 October 2024, question 2.

⁴⁸³ Agreed minutes of meeting with [third-party developer] of 12 November 2024, paragraph 16.

⁴⁸⁴ Technical meeting [third-party developer]/Commission of 12 November 2024, slide deck page 7.

⁴⁸⁵ Technical meeting [third-party developer]/Commission of 12 November 2024, slide deck page 7.

- (453) A casting solution must have the ability to cast media and control ongoing casting sessions with sufficient resources – including in the background, without the app or solution from which an item was shared having to be open in the foreground. For example, screen mirroring must not face any crashes due to resource exhaustion even if running long-term, continue when the initiating app is closed, and when casting video to a TV, the casting should not stop when the iOS device is locked.

5.9.2. *Feature falls within the scope of Article 6(7) of Regulation (EU) 2022/1925*

- (454) The Commission finds that features for media casting as described in Section 5.9.1 of this Decision – together with their functionalities – fall within the scope of Article 6(7) of Regulation (EU) 2022/1925. Media casting is enabled via software and hardware features which are controlled via iOS, Apple’s operating systems for iPhones, which is listed in the Designation Decision.

5.9.3. *Current implementation for Apple’s own services and hardware*

- (455) The features relating to media casting are currently used by Apple for its own services and hardware. For instance, Apple’s casting solution AirPlay comes pre-installed on Apple devices. AirPlay, as well as several other functionalities provided by Apple, rely on the media casting features discussed in this section. Functionalities currently used by Apple’s services and hardware are listed below.

- (a) Accessibility. Convenient access to functionality via the iOS Control Centre is used by several Apple services and connected physical devices. For instance, AirPlay can be initiated directly from the iOS Control Centre, which a user can access at any time. Apple connected physical devices also enjoy deep integration in the iOS Control Centre. For example, Apple headphone features, such as noise cancelling and conversation awareness, can be toggled directly under the volume setting.
- (b) Centralised availability. Apple habitually integrates its first-party solutions in a central place in the iOS, from where all developers can call upon them for seamless integration in their iPhone apps with only a few lines of code (or even by default). For example, this is the case for both AirPlay and AirDrop.
- (c) Advertisement and discovery. Advertisement and discovery are used for Apple services that require connection to another device. For instance, AirDrop uses it to identify devices available for file transfer, and AirPlay uses it to identify AirPlay-compatible receiving devices. Apple’s own connected physical devices use multiple technologies for advertisement and discovery, such as BLE for AirDrop and AirPlay, AWDL and NFC for AirDrop, or UWB for AirPlay on HomePod.⁴⁸⁶
- (d) Communication protocols. Communication protocols such as P2P Wi-Fi are used by Apple services to transmit data directly to other devices at high speed. AirDrop uses communication protocols, including P2P Wi-Fi, to transfer files and AirPlay uses it to stream media to another device. Apple connected physical devices, such as Apple TV or Apple Vision Pro, also use

⁴⁸⁶ See <https://www.theverge.com/2021/1/26/22250856/homepod-mini-ultra-wideband-handoff-feature-update-ios-14-apple-iphone-u1>, accessed on 15 November 2024.

communication protocols including P2P Wi-Fi to communicate with iOS devices. [...]⁴⁸⁷

- (e) Controls. The hardware control buttons, as well as on-screen buttons on the lock screen are used by Apple services to control media playback. For instance, AirPlay casting sessions can be controlled this way, as well as music playing on an Apple connected physical device (e.g. headphones).

(456) Apple's connected physical devices and apps have background execution privileges that ensure that they continue operating when the relevant app is not running in the foreground. Apple can execute casting in the background on iOS devices through a privileged background process that is only available to Apple.⁴⁸⁸ This feature is described in detail in Section 5.6 of this Decision. [...]⁴⁸⁹

5.9.4. *Current implementation for third-party services and hardware*

(457) Apple provides frameworks that third-party developers can use to implement media casting functionalities in their apps. Some third parties may use these tools to build app-specific media casting solutions, but other third parties use these tools to develop a generic casting solution which they make available to other third parties through a software development kit (e.g. Google Cast). These software development kits, to the extent supported by iOS, can be integrated in an app to allow it to cast media to compatible receiver devices.

(458) For example, the *ReplayKit* framework⁴⁹⁰ allows developers to capture the screen and audio from the iPhone, which can subsequently be recorded or broadcast. *ReplayKit* does not allow capturing and casting of digital rights management ("DRM")-protected content.⁴⁹¹ *ReplayKit* can be used by third parties to implement screen mirroring functionality, similar to AirPlay screen mirroring. Each screen mirroring app is required to create its own broadcast extension.⁴⁹² Developers have used this framework to develop screen mirroring apps for iOS.⁴⁹³

(459) The frameworks and APIs available to third parties for building media casting solutions show several shortcomings compared to Apple's own media casting solution AirPlay.

(460) *First*, in terms of accessibility, third party casting solutions do not enjoy the same accessibility as Apple AirPlay. AirPlay is available directly in the iOS Control Centre, as well as in in-app picking menus. While a third-party app developer can make the third-party casting solutions that they integrated into their app available in the same picking menu as AirPlay within their own apps using the *DeviceDiscoveryExtension* framework,⁴⁹⁴ third-party casting solutions are not available in the Control Centre picking menu. This may create confusion for users on

⁴⁸⁷ Apple's reply to RFI 6 of 23 October 2024, Annex Q24.3, page 21.

⁴⁸⁸ The Commission understands that AirPlay casting is supported by an iOS daemon, an iOS process which allows to execute actions in the background (Section 5.6.3 of this Decision). See Apple's internal documents [...].

⁴⁸⁹ Apple's reply to RFI 6 of 23 October 2024, question 34.

⁴⁹⁰ See <https://developer.apple.com/documentation/replaykit/>, accessed on 5 November 2024.

⁴⁹¹ Apple's internal document [...].

⁴⁹² See <https://support.apple.com/guide/security/replaykit-security-seca5fc039dd/web>, accessed on 15 November 2024.

⁴⁹³ See, for example, <https://screenmirroring.app/>, accessed on 5 November 2024.

⁴⁹⁴ Apple's reply to RFI 5 of 16 October 2024, questions 1 to 3.

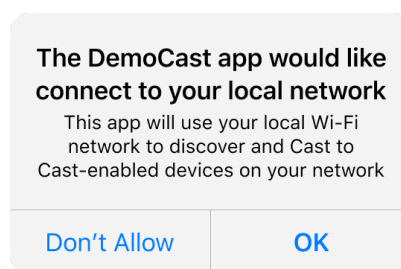
how to initiate casting with a third-party casting solution. Specifically for screen mirroring, AirPlay features a prominent button directly in the iPhone's Control Centre, while screen mirroring implementations via ReplayKit are only accessible via the relevant app. This causes friction and may be confusing to users as screen mirroring functionality is expected to be accessible under the screen mirroring dialog in the iOS Control Centre.

- (461) *Second*, app developers are required to fully integrate the third-party casting SDK in their own app. This requires additional development effort compared to AirPlay integration, including to discover such third-party casting solutions, consult their documentation, and integrate one or potentially more into their development and build process.⁴⁹⁵ This process must be repeated for each third-party casting solution that the app developer desires to support. In contrast, if an app developer uses standard media playback APIs, audio and video content can be casted automatically through AirPlay using the picker in the iOS Control Centre unless the developer explicitly disables this.⁴⁹⁶
- (462) *Third*, since every app must integrate the third-party casting SDK separately, the SDK also increases the size of the app; the SDK may exist in many duplicate copies across third-party apps, unnecessarily using storage space; and the SDK cannot be updated centrally and instead may be outdated if a developer fails to update their app, leading to an inconsistent user experience across apps, and possibly leave security vulnerabilities unaddressed. In contrast, AirPlay is integrated within iOS, therefore existing only in one copy, and is automatically updated together with iOS for all third-party apps using AirPlay.
- (463) *Fourth*, in terms of advertisement and discovery, discovery of casting targets for third-party casting solutions is not equivalent to AirPlay, inhibiting seamless discovery and reliable connection to initiate casting. Due to the lack of P2P Wi-Fi for third parties (see Section 5.4 of this Decision), the user must enable local network access for the relevant app so that it can discover devices to cast to, using infrastructure Wi-Fi. These devices must be on the same local network. Furthermore, when casting for the first time, a warning prompt is shown during device discovery which is not shown in the case of AirPlay.
- (464) Third parties also do not have access to proximity hardware, such as UWB, which AirPlay uses to enable seamless connection to Apple hardware such as the HomePod.

⁴⁹⁵ Agreed minutes of meeting with [third-party developer] of 29 October 2024, paragraph 9.

⁴⁹⁶ Apple's reply to RFI 5 of 16 October 2024, question 11. [...] See also, for example the "allowsExternalPlayback" property of AVPlayer at <https://developer.apple.com/documentation/avfoundation/avplayer/1387441-allowsexternalplayback>: "A Boolean value that indicates whether the player allows switching to external playback mode" where "The default value of this property is true," accessed on 5 November 2024.

Figure 19: Warning prompt during device discovery



Source: https://developers.google.com/cast/docs/ios_sender, accessed on 18 November 2024.

- (465) *Fifth*, in terms of communication protocols, third-party casting solutions do not have access to the same high-bandwidth communication methods as AirPlay, which allow to cast content at high resolution and with low latency. AirPlay is able to maintain an AWDL connection, Apple’s proprietary P2P Wi-Fi protocol, directly between the iPhone and the connected physical device. In addition to the high bandwidth offered by P2P Wi-Fi, it also means that the iPhone and connected physical device do not need to be connected to the same local network to cast. As set out in Section 5.4 of this Decision, Apple does not currently make P2P Wi-Fi available to third parties on iOS.
- (466) *Sixth*, in terms of controls, third-party casting solutions are also not able to use the physical volume buttons to control the volume of the casting session.⁴⁹⁷
- (467) *Seventh*, [...]. If that limit is exceeded, the mirroring session crashes, and an iOS error message is shown to the end user. This limit is sufficiently low to require trade-offs regarding video quality to avoid crashes. Apple has not increased this limit over the past years as more powerful iOS devices have been released.⁴⁹⁸
- (468) *Eighth*, in terms of general interoperability, third-party casting solutions face several other hurdles, which each make the experience less seamless than AirPlay. For instance, when initiating screen mirroring via ReplayKit, a warning screen is shown explaining that everything on the screen, including notifications, will be recorded. This message can cause confusion for users as they may not understand why the app “records” the screen to mirror the screen. This may require explanations on the part of the app developer, cluttering the user interface. Furthermore, when initiating screen mirroring via an app based on ReplayKit, the user has to select a “broadcast extension” from a list. This can lead to confusion for the user in case multiple screen mirroring apps are installed on the iPhone. Altogether, initiating screen mirroring via an app that uses ReplayKit is therefore more burdensome than initiating AirPlay screen mirroring.⁴⁹⁹
- (469) Therefore, the Commission considers that there is currently an interoperability gap when it comes to third-party connected physical devices connected to iOS devices and that it should specify how Apple has to fill this gap to comply with Article 6(7) of Regulation (EU) 2022/1925.

⁴⁹⁷ See https://developers.google.com/cast/docs/ios_sender/integrate, accessed on 5 November 2024.

⁴⁹⁸ [Third-party developer]’s reply to RFI of 16 October 2024, question 3.

⁴⁹⁹ [Third-party developer]’s reply to RFI of 16 October 2024, question 3.

5.9.5. *The gatekeeper's view*

- (470) *First*, Apple submits that the relevant iOS feature is media casting, and that accessibility, centralised availability, advertisement and discovery, communication protocols, controls and execution cannot be considered separate features, as they offer no independent functionalities to users outside of the context of media casting.⁵⁰⁰
- (471) *Second*, Apple submits that it already provides effective interoperability with media casting. Apple points out that there are already third parties today that offer media casting solutions for iOS. [...] ⁵⁰¹
- (472) *Third*, Apple argues that the measures set out in the Preliminary Findings go beyond what is needed for effective interoperability for media casting, as the legal test does not require Apple to provide equal conditions on each aspect set out in the Preliminary Findings.⁵⁰²
- (473) *Fourth*, Apple argues that centralised availability is not required for effective interoperability, requiring it would be disproportionate, and raises integrity concerns. Apple argues that the need for centralised availability has not been assessed rigorously in the Preliminary Findings, as it lacks quantification and relies on thin evidence. Apple further submits that the Preliminary Findings fail to consider that Article 6(7) of Regulation (EU) 2022/1925 serves to promote innovation, and not promote free riding on Apple's innovation.⁵⁰³
- (474) *Fifth*, Apple submits that the measures set out in the Preliminary Findings relating to advertisement and discovery are not necessary for effective interoperability. Apple indicates that the Preliminary Findings identify no relevant interoperability concerns relating to making the iPhone discoverable by third-party devices.⁵⁰⁴
- (475) *Sixth*, Apple submits that the measures set out in the Preliminary Findings relating to communications protocols are not necessary for effective interoperability. Apple indicates [...], and that NFC and UWB are not required. [...] ⁵⁰⁵
- (476) *Seventh*, Apple submits that the measures in the Preliminary Findings relating to execution are not necessary for effective interoperability. It also submits that the interoperability issues in this area set out in the Preliminary Findings rely on statements from a single developer.⁵⁰⁶
- (477) *Eighth*, Apple submits that the measures in the Preliminary Findings relating to warning screens and prompts are not necessary for interoperability. Apple argues that

⁵⁰⁰ Apple's reply to the Preliminary Findings, paragraphs 267-268 and Apple's submission of 24 October 2024.

⁵⁰¹ Apple's reply to the Preliminary Findings, paragraphs 269-273.

⁵⁰² Apple's reply to the Preliminary Findings, paragraph 274.

⁵⁰³ Apple's reply to the Preliminary Findings, paragraphs 275-281; Apple's mark-up of the Commission's proposed measures of 23 January, paragraph (96)(b).

⁵⁰⁴ Apple's reply to the Preliminary Findings, paragraphs 282-284; Apple's mark-up of the Commission's proposed measures dated 23 January 2025, paragraph (96)(c). See also Email from Apple to the Commission on 13 February 2025 [on the draft final measures].

⁵⁰⁵ Apple's reply to the Preliminary Findings, paragraph 285; Apple's mark-up of the Commission's proposed measures of 23 January, paragraph (96)(d); Email from Apple to the Commission on 13 February 2025 [on the draft final measures].

⁵⁰⁶ Apple's reply to the Preliminary Findings, paragraphs 286-288; Apple's mark-up of the Commission's proposed measures of 23 January, paragraph (96)(f).

the Preliminary Findings fail to identify prompts that would render interoperability ineffective, and do not quantify the effects of the prompts identified. Apple submits that prompts can be necessary and proportionate integrity measures.⁵⁰⁷

- (478) *Ninth*, Apple argues that the requirement set out in the Preliminary Findings that new features and updates to AirPlay must be made available to third-party casting solutions is unnecessary for effective interoperability, as they do not render interoperability ineffective.⁵⁰⁸
- (479) *Tenth*, Apple submits that the implementation timing proposed in the Preliminary Findings is not feasible.⁵⁰⁹ In a later submission, [...] ⁵¹⁰
- (480) [...] ⁵¹¹ [...] ⁵¹²

5.9.6. *The Commission's assessment*

5.9.6.1. Concerning media casting comprising several relevant features

- (481) Apple argues that the elements in recital (452) of this Decision are not features in their own right and that instead media casting overall is the relevant feature. However, each of the elements described under recital (452) of this Decision is required to enable interoperability for media casting under equal conditions to Apple. A narrower definition would not achieve interoperability under equal conditions to Apple, as third parties would continue to face obstacles not faced by Apple.
- (482) It is also inaccurate for Apple to contend that none of these elements offer independent functionalities outside of the context of media casting. Several of them show up in other solutions that are covered in this Decision: for example, Apple's close-range wireless file sharing solution uses the features of accessibility, advertisement and discovery, and communication protocols.⁵¹³ One communication protocol, high-bandwidth peer-to-peer Wi-Fi, is even a self-standing feature within this Decision.⁵¹⁴ Clearly, the features for media casting therefore offer independent functionality beyond media casting alone.
- (483) In any event, even if the relevant feature were media casting, and not the elements of media casting described in recital (452) of this Decision (*quod non*), the Commission considers that this distinction does not make any difference with regard to Apple's interoperability obligations. Apple is still required to provide effective interoperability with each functionality of a given feature, since it is required, under Article 6(7) of Regulation (EU) 2022/1925, to provide full and effective interoperability under equal conditions to the said feature, which consists of one or several functionalities. As explained in Section 3.1.1 of this Decision, the Commission is not required to demonstrate that each of the measures are necessary to enable contestability, i.e. that (some) third parties are able to provide a "*competitive offering*" or an "*alternative solution*" which is enough for achieving contestability.

⁵⁰⁷ Apple's reply to the Preliminary Findings, paragraphs 289-294; Apple's mark-up of the Commission's proposed measures of 23 January, paragraph (97)(c).

⁵⁰⁸ Apple's reply to the Preliminary Findings, paragraph 295; Apple's mark-up of the Commission's proposed measures of 23 January, paragraph (99).

⁵⁰⁹ Apple's reply to the Preliminary Findings, paragraphs 296-297.

⁵¹⁰ Email from Apple to the Commission of 3 February 2025.

⁵¹¹ Apple's submissions of 7 November 2024; Apple's submission of 15 November 2024.

⁵¹² Apple's submission of 28 January 2025.

⁵¹³ See Section 5.7 of this Decision.

⁵¹⁴ See Section 5.4 of this Decision.

Such assessment would re-import the requirement to investigate on a case-by-case basis the effects on competition of a gatekeeper's given conduct, which the legislator explicitly rejected and is contrary to the text and purpose of Article 6(7) of Regulation (EU) 2022/1925. Moreover, it would effectively relieve Apple of the burden of demonstrating compliance under Article 8(1) of Regulation (EU) 2022/1925. Under the correct legal test, the measures therefore do not go beyond what is necessary for effective interoperability regardless of whether media casting is a single feature or a set of features.

5.9.6.2. Concerning interoperability gaps with regard to media casting

(484) Apple claims that it already provides effective interoperability for media casting. To support this claim, it highlights the existence of third-party casting solutions, notably Google Cast. It also highlights that several media apps support multiple casting solutions.

(485) However, [third-party developer] has pointed out several shortcomings [...] when interoperating with iOS, including restrictions on data transfer and lack of system access for centralised availability and use of shared storage.⁵¹⁵ This clearly shows that while third parties are able to offer casting solutions on iOS, they do not enjoy equal conditions to AirPlay. Apple tries to downplay these shortcomings by characterising [third-party developer]'s feedback as “*manifestly self-serving*.”⁵¹⁶ However, Apple does not contest the existence of these shortcomings – it only claims that the Commission should have quantified their impact.⁵¹⁷ The Commission disagrees with Apple's interpretation of the legal standard on which its argument is predicated (see recital (483) of this Decision).

(486) [...] ⁵¹⁸ [...]

5.9.6.3. Concerning centralised availability being a proportionate measure, required for effective interoperability, and consistent with the integrity justification

(487) Apple asserts that the measure to require centralised availability of third-party casting solutions is disproportionate and not based on meaningful evidence. For instance, on the Commission's meeting with [third-party developer], Apple says that “*it is not clear from the minutes on which experience [third-party developer]'s statements are based.*”⁵¹⁹ This statement, questioning [third-party developer]'s expertise, is surprising, as [third-party developer] has been recognised by Apple multiple times for responsible disclosure of iOS security vulnerabilities⁵²⁰ and [third party developer]'s publications were referenced by Apple in multiple RFI responses during the proceedings.⁵²¹

⁵¹⁵ Technical meeting [third-party developer]/Commission of 12 November 2024, slide deck page 7.

⁵¹⁶ Apple's reply to the Preliminary Findings, paragraph 278.

⁵¹⁷ In its reply to the Preliminary Findings, Apple only tries to rebut [third-party developer]'s statement that “*some app developers choose not to include Cast functionality into their app*” by giving three examples of major media streaming apps that did choose to include Cast functionality. These few examples do not invalidate [third-party developer]'s statement.

⁵¹⁸ Apple's reply to the Preliminary Findings, paragraph 273.

⁵¹⁹ Apple's reply to the Preliminary Findings, paragraph 277.

⁵²⁰ See, for instance, [...].

⁵²¹ Apple's Reply to RFI 3 of 7 October 2024, footnote 2; Apple's Reply to RFI 5 of 16 October 2024, footnotes 27, 28 and 29.

- (488) Apple goes on to dismiss [third-party developer]’s feedback as self-serving.⁵²² However, as the provider of a major third-party casting solution, it is difficult to understand how [third-party developer]’s feedback would not be relevant (see recital (485) of this Decision). Apple suggests that the Commission should have done a survey among developers on this topic instead. The Commission conducted a public consultation on the proposed measures, which attracted positive feedback from developers.
- (489) Apple further submits that the measures concerning centralised availability allow third parties to free ride on Apple’s investments as it removes the need for third parties to invest in their own development.⁵²³ This assertion is misguided, as centralised availability is currently impossible for third parties to develop on their own, as interoperability with the relevant iOS features is currently prevented by Apple. In fact, having centralised availability will not reduce the development or investment needed by a third-party casting solution provider to provide a functional and feature-rich media casting solution – it simply addresses the disadvantages that third parties face compared to Apple due the pre-installation of AirPlay. Today, each media app that wishes to use a third-party casting solution must implement the relevant code in their app. Centralised availability ensures that this is no longer necessary, and that casting solutions installed by the user can be accessed centrally, as is the case for Apple’s AirPlay. Third-party casting solutions will have to expend the same development effort as Apple. Therefore, there is no free riding. In fact, as set out in recital (98) of this Decision, the measures specified by the Commission will indirectly increase Apple’s incentives to innovate within iOS.
- (490) Apple argues that there is no evidence to support that casting solutions need to be supported by hundreds of apps for contestability. Apple explains that the three largest video-on-demand apps make up the majority of the subscription video-on-demand market.⁵²⁴ However, the fact remains that third-party casting solutions currently must convince each relevant app developer to integrate the casting solution into their apps – a step that is not required for Apple’s AirPlay. Media casting is relevant to far more types of apps than the narrow segment of “subscription video-on-demand” apps that Apple uses as an example. Any app that streams media could be relevant.
- (491) Apple claims that allowing centralised availability for third-party casting solutions would raise integrity concerns.⁵²⁵ [...] This explanation does not meet the threshold to duly justify integrity concerns. Moreover, examples where iOS apps do share code already exist today, most notably Apple’s App Extensions.⁵²⁶ App Extensions is a model through which Apple allows third-party apps to expose functionality to other apps – a mechanism that is very similar to the centralised availability included in the media casting measures. [...] ⁵²⁷ [...] Apple therefore does not appear to raise integrity concerns. In any case, Apple does not duly substantiate their concerns to the standard set out in Section 3.3 of this Decision and Apple’s concerns do not affect the feasibility of providing interoperability with the centralised availability feature, i.e. Apple does not argue that it cannot technically implement an interoperability

⁵²² Apple’s reply to the Preliminary Findings, paragraph 278.

⁵²³ Apple’s reply to the Preliminary Findings, paragraph 279.

⁵²⁴ Apple’s reply to the Preliminary Findings, paragraph 243.

⁵²⁵ Apple’s reply to the Preliminary Findings, paragraph 280.

⁵²⁶ See <https://developer.apple.com/app-extensions/>, accessed on 18 February 2025.

⁵²⁷ Apple’s submission of 28 January 2025.

solution for this feature. Any integrity issue should thus be limited to the implementation phase, i.e. the adjustments under which that solution is made available to third parties.⁵²⁸

- (492) Finally, Apple argues that media streaming apps are not required to integrate a third-party media solution but can choose to develop their own – thereby removing the need for centralised availability.⁵²⁹ This argument disregards the clear issues relating to network effects set out in the Preliminary Findings.⁵³⁰ While some major media player apps may choose to develop a custom casting protocol, this is not in reach for the typical app developer. The single app would not enjoy sufficient adoption among receiving devices – such as smart TVs – to be attractive to end users. Conversely, achieving adoption among receiving devices for a casting protocol that is specific to a single media player app would be an uphill battle, compared to a media casting solution that is used across apps (and therefore by many end users).

5.9.6.4. Concerning measures relating to advertisement and discoverability being necessary and proportionate

- (493) Apple submits that the Commission presents no evidence that access to proximity hardware such as UWB is required for effective interoperability.⁵³¹ This is inaccurate, as this was a shortcoming highlighted by [third-party developer], the provider of a major casting solution. It is also a method of device discovery that is used by Apple's AirPlay – for instance as a way of initiating audio streaming to a HomePod.⁵³² Third parties therefore require access to proximity hardware to enjoy interoperability under equal conditions. Apple's position that access to proximity hardware is not necessary for effective interoperability is predicated on its misrepresentation of the legal standard of Article 6(7) of Regulation (EU) 2022/1925 (see recital (483) of this Decision). Under the correct legal test, the measures therefore do not go beyond what is necessary for effective interoperability.
- (494) Apple furthermore submits that the Commission does not identify relevant interoperability concerns in relation to making the iPhone discoverable by third-party devices as a receiving device and indicates that receiving media streams on the iPhone is not a common use case.⁵³³ However, at least one third party indicated to the Commission that it faces serious obstacles in this respect.⁵³⁴ Apple also received an interoperability request which covers this issue in March 2024.⁵³⁵ In any event, even if there was no interoperability gap in this respect (*quod non*), the Commission can still specify measures relating to iPhone discoverability. Discoverability is an important feature within media casting and must be covered for the measures to be complete and for interoperability to be full and effective. The relevance of iPhone discoverability is demonstrated by the fact that it is a use case that is relevant, and used by Apple, for its virtual reality headsets, a technology that is on the rise.

⁵²⁸ Agreed minutes of meetings with Apple on 11 and 12 February 2025.

⁵²⁹ Apple's reply to the Preliminary Findings, paragraph 281.

⁵³⁰ Preliminary Findings, paragraph 269.

⁵³¹ Apple's reply to the Preliminary Findings, paragraph 283.

⁵³² See <https://support.apple.com/en-tm/guide/homepod/apdfb81a72e4>, accessed on 18 February 2025.

⁵³³ Apple's reply to the Preliminary Findings, paragraph 284.

⁵³⁴ Non-confidential agreed minutes of call with [third-party developer] of 21 October 2024, paragraph 8.

⁵³⁵ Request submitted by [third-party developer] on 9 March 2024 through the Interoperability Request Portal. Apple and [third-party developer] had several interactions to clarify the request.

5.9.6.5. Concerning measures relating to communication protocols being necessary and proportionate

(495) [...] ⁵³⁶ However, Apple’s statement concerning NFC and UWB is misleading. While they may not be used as a *transport* protocol for the content stream, proximity hardware is used to initiate connections with Apple connected physical devices (see Section 5.9.6.4 of this Decision) and is therefore a relevant communication protocol in the context of media casting. ⁵³⁷

(496) [...] Furthermore, the Commission’s measures for media casting are not limited to areas for which interoperability gaps exist. Instead, the measures cover media casting as a whole – including areas where interoperability may already be available today.

5.9.6.6. Concerning measures relating to execution being necessary and proportionate

(497) Apple submits that giving third-party casting solutions access to the same system resources as AirPlay is not necessary to achieve “*effective interoperability*,” under Apple’s understanding of the legal standard. ⁵³⁸ As explained in Section 3.1.1 of this Decision, the Commission disagrees with this interpretation of the legal standard. (see recital (483) of this Decision). Under the correct legal test, the measures do not go beyond what is necessary for effective interoperability.

(498) Apple claims that the Preliminary Findings do not identify relevant shortcomings in the area of execution, and in particular that the existence of “*trade-offs regarding video quality to avoid crashes*” is insufficient to render interoperability ineffective. Apple also claims that the statement stems from a single developer, and not a broader survey of the developer community. ⁵³⁹ [...] Apple’s claim that this does not render interoperability ineffective is not justified and based on Apple’s misrepresentation of the legal standard (see recital (483) of this Decision). Furthermore, the developer that gave this feedback markets a screen mirroring app that Apple presented to the Commission as an example of existing third-party solutions. ⁵⁴⁰ The Commission contacted this developer following that presentation to understand whether it faced any interoperability issues with its app. ⁵⁴¹ It is therefore hard to understand on which basis Apple dismisses this finding as an “*unfounded assertion*.”

5.9.6.7. Concerning the user journey for third-party casting solutions having to be equally effective to that of Apple

(499) Apple submits that the Commission’s Preliminary Findings do not identify warning screens or prompts that would make interoperability for media casting ineffective. Apple also submits that prompts can be strictly necessary and proportionate integrity measures. ⁵⁴²

(500) As recalled in recitals (85)-(86), and in line with the requirements of Article 13(4) and (6) of Regulation (EU) 2022/1925, warning screens and prompts should not unduly compromise the user experience that third parties can provide when

⁵³⁶ Apple’s reply to the Preliminary Findings, paragraph 285; Email from Apple to the Commission on 13 February 2025 [on the draft final measures].

⁵³⁷ Apple internal document [...].

⁵³⁸ Apple’s reply to the Preliminary Findings, paragraph 287.

⁵³⁹ Apple’s reply to the Preliminary Findings, paragraph 288.

⁵⁴⁰ Technical meeting Apple/Commission of 14 October 2024, AirPlay slide deck page 11.

⁵⁴¹ [Third-party developer]’s reply to RFI of 16 October 2024.

⁵⁴² Apple’s reply to the Preliminary Findings, paragraphs 290-294.

compared to Apple. For instance, prompts should not be unnecessarily frequent or intrusive, or employ non-neutral or leading language, misleading design patterns (so-called dark patterns) or misrepresent the risks of granting permission. Accordingly, while the Commission does not object to prompts and warnings as such, the conditions under which these are implemented can affect effective interoperability.

5.9.6.8. Concerning Apple having to allow interoperability for future media casting functionalities

- (501) Apple's argument that Article 6(7) of Regulation (EU) 2022/1925 does not require it to give access to future media casting functionalities cannot be accepted. As set out in Section 3.1.1 of this Decision, Apple does not clarify at what point it intends to provide interoperability for new functionalities to third parties. In the case of media casting, this issue is particularly acute. If Apple were allowed to introduce new capabilities to AirPlay on the basis of media casting features that are not available to third-party media casting solutions, this would obstruct the ability of third parties to offer competitive media casting solution on iOS and stymie innovation.
- (502) Furthermore, as explained in Section 3.1.1 of this Decision, this would not deprive Apple of its incentives to innovate and competitive advantage. Competing media casting protocols cannot free ride on innovations in AirPlay – they simply require access to iOS capabilities under the same conditions to be able to implement their own functionalities and compete with AirPlay. Third-party casting solutions will have to expend the same development effort as Apple.

5.9.6.9. Concerning timing

- (503) Apple submits that the implementation timing for media casting proposed in the Preliminary Findings is not feasible due to Apple's software development cycle. Apple argues that it cannot rely on its existing first-party media casting solution, AirPlay, but needs to develop new solutions to allow interoperability, which requires more time.⁵⁴³ [...] ⁵⁴⁴
- (504) The Commission considers that Regulation (EU) 2022/1925 does not require Apple to develop new solutions to enable interoperability for media casting. It is Apple's choice to do so, rather than to open the interfaces that Apple uses itself, e.g. for AirPlay. [...]

5.9.7. *Measures that Apple should implement*

- (505) To meet the requirements of Article 6(7) of Regulation (EU) 2022/1925, Apple should implement an interoperability solution that provides third parties with access to the same features for media casting as available to Apple (as described in Section 5.9.1 of this Decision), in a way that is equally effective as the solution available to Apple.
- (506) Apple should implement an interoperability solution that provides third parties with access to the same features for media casting described in Section 5.9.1 of this Decision as available to Apple and its connected physical devices, including, but not limited to, Apple Watch, Apple Vision Pro, as well as any future Apple connected physical devices. Apple should allow third parties effective interoperability in a way that is equally effective as the solution available to Apple. In particular, Apple should

⁵⁴³ Apple's reply to the Preliminary Findings, paragraphs 296-297.

⁵⁴⁴ Email from Apple to the Commission of 3 February 2025.

allow effective interoperability with the iOS features used by Apple's media casting solutions, such as AirPlay. To that end, Apple should make the following features available to third-party casting solutions.

- (a) Accessibility. Apple should allow the casting solution to be selectable in the same in-app picking menu as is used for AirPlay in supported apps. The casting solution must also be selectable directly from the iOS Control Centre picker as is used for AirPlay. The end user should be able to initiate and use the casting solution without the need to open the third-party casting app in the foreground, and in the case of using the iOS Control Centre picker without the need to open the media app in the foreground.
 - (b) Centralised availability. Apple should allow third parties to centrally provide their casting solution on iOS, e.g. through an extension, such that end users who install the casting solution can access the third-party casting provider in any app that uses standard media playback APIs without the need for the app developer to integrate an SDK in their apps.
 - (c) Advertisement and discovery. Apple should make available device discovery that allows compatible third-party devices to be discoverable on the iPhone, enabling that the sender iPhone device shows these receivers in the casting pickers in the system user interface and in apps, and make the iPhone discoverable by third-party devices, by enabling sender devices to listen for the iPhone's capabilities as a receiver.
 - (d) Communication protocols: Apple should allow third parties to make available the same communication protocols that are available to Apple's casting solutions, such as AirPlay. This includes but is not limited to Bluetooth, Infrastructure Wi-Fi, P2P Wi-Fi, and UWB. Apple should allow third parties to switch between available communication protocols and to access the required information to select the most suitable protocol. Apple should allow third parties to integrate their media streaming protocols based on communication protocols.
 - (e) Controls. Apple should allow the third parties to implement the same hardware button functionality (e.g. volume controls) and lock screen controls (e.g. pause, fast forward, etc.) that are available to Apple's casting solutions, such as AirPlay.
- (507) Interoperability for third-party casting solutions must be effective. To this end, Apple should:
- (a) not impose limits or restrictions that may affect the audio, image or video quality achievable by third-party media casting solutions, such as inaccessibility of communication protocols, background execution restrictions, memory consumption bandwidth limits, or limits on other system resources, to the extent that these are not imposed on AirPlay; and
 - (b) allow media casting solutions to use third-party DRM systems. Apple should not impose restrictions concerning the casting of DRM-protected content that go beyond those imposed on AirPlay.
- (508) Apple should grant third parties access to additional functionalities if necessary to enable effective interoperability with the features for media casting described in Section 5.9.1 of this Decision.

- (509) For the purpose of ensuring that effective interoperability continues in the future, third parties must also have access to any future updates, including new functionalities, of the media casting features insofar and as soon as they are available to Apple's AirPlay. For example, if Apple updates AirPlay to stream video at higher resolution, or to allow end users to initiate screen mirroring via an AI assistant, third party casting solutions should be provided the necessary interoperability to implement these functionalities as well. To this end, the general measures in Section 5.12 of this Decision apply, including in particular the measures concerning future updates and new functionalities set out in Section 5.12.7 in this Decision.

5.9.8. Implementation timing

- (510) Apple should implement all measures to provide effective interoperability with the iOS features for media casting in the release of iOS 20, and in any case by the end of 2026 at the latest.

5.10. Measures for automatic audio switching

- (511) The automatic audio switching feature on iOS devices allows wireless headphones to automatically switch the audio source from one Apple device, including iOS devices, to another Apple device that is playing audio. For instance, if a user listens to music on their Apple AirPods, which are playing audio input from the end user's iPad, but the end user receives a phone call on their iPhone, the iPhone will take over the audio connection to the AirPods, recognising both, that the phone call likely has priority over the music and that the AirPods are in use.
- (512) Third parties do not enjoy the same level of interoperability for automatic audio switching. iOS does not provide third-party headphones with information from iOS to accurately determine what type of audio either source device is sending. Therefore, those third-party headphones cannot achieve the functionality in switching audio sources based on information about the audio source (e.g. phone call versus music) as Apple headphones can. iOS also does not provide a way for third-party headphones to submit information to iOS to accurately determine where audio should be routed to. Third-party headphone developers could exchange that information to enable and improve automatic audio switching between an iOS device and another Apple device, and between an iOS device and third-party devices. This lack of access to iOS leaves end users of third-party headphones with a worse experience than end users with Apple headphones, thereby preventing a level playing field.

5.10.1. Description of the feature

- (513) On iOS devices, audio content, including but not limited to music and phone calls, can be broadcast to connected physical devices, such as wireless headphones. To broadcast audio content from an iOS device to headphones, the headphones must be paired with the iOS device via Bluetooth.
- (514) Once an active Bluetooth connection between the wireless headphones and an iOS device is established, audio content can generally only be broadcast from that one iOS device to the connected wireless headphones. Before audio can be broadcast from a different iOS device, the existing Bluetooth connection of the wireless headphones with the first iOS device must be disconnected and a new active Bluetooth connection must be established with the second iOS device.
- (515) Instead of requiring a user to manually choose which device should broadcast audio to their headphones, the automatic audio switching feature allows end users with

Apple's own headphones to automatically switch between the audio source (i.e. active Bluetooth connection) of two different Apple devices (including iOS devices). On the audio source side, automatic audio switching is supported on iPhones, iPads, Macs and to a limited extent on Apple Watches.⁵⁴⁵ On the headphone side, automatic audio switching is supported on several Apple headphone models, such as AirPods and Beats.⁵⁴⁶

- (516) On Apple devices, automatic audio switching is activated when a secondary audio-broadcasting device that is within Bluetooth range of paired headphones, which already stream audio from the primary audio-broadcasting device, starts playing audio. The secondary device makes a Bluetooth audio request to the headphones. The headphones respond to the secondary device with data provided by the primary device, enabling the secondary device to determine whether its audio session has priority over the primary device's audio session. If so, the secondary device's audio will take over and play through the headphones, while the primary device will stream its audio from its built-in speaker.⁵⁴⁷ If a third device becomes active, it compares its activity level to the activity level of the secondary device [...].⁵⁴⁸
- (517) For example, if the end user is listening to music through AirPods on one iOS device but starts a phone call from a different iOS device, the automatic audio switching feature will automatically connect the AirPods to the iOS device on which the phone call is being made from.
- (518) Automatic audio switching on Apple devices relies on certain information from Apple and third-party apps on iOS, and from iOS. Apple submits that apps specify the relevant audio type (e.g. media, call, notification) when they start an audio session.⁵⁴⁹ iOS then makes this information available to the headphones. Relevant information also includes information on the current audio route (e.g. local speakers, wired headphones, wireless headphones, car), the reason for selecting the current audio source (e.g. user action, iOS decision), and information on the upcoming audio source.⁵⁵⁰ The feature can also rely on information fed from the headphones (or other audio output) to the audio source. For instance, AirPods can tell an iPhone whether they are in-ear or not.⁵⁵¹
- (519) Another important aspect of the audio switching feature is audio routing. Audio routing is the set of policies that iOS applies to determine to which audio output each type of audio should be routed to. For instance, when accepting a phone call with the interface on the iPhone screen with your AirPods connected and in-ear, the audio will automatically be routed to the AirPods. This is not the case for third-party headphones – in this case the audio is routed to the iPhone speakers instead.⁵⁵²

⁵⁴⁵ Apple's reply to RFI 3 of 7 October 2024, question 48.

⁵⁴⁶ AirPods 2, 3, and 4; AirPods Pro 1 and 2; AirPods Max and certain Beats headphones. See Apple's reply to RFI 3 of 7 October 2024, question 49.

⁵⁴⁷ Apple's reply to RFI 3 of 7 October 2024, question 50.

⁵⁴⁸ Apple's reply to RFI 3 of 7 October 2024, question 48.

⁵⁴⁹ Apple's reply to RFI 3 of 7 October 2024, question 51.

⁵⁵⁰ [Third-party developer]'s reply to RFI 2 of 25 October 2024, paragraph 23.1.

⁵⁵¹ See <https://support.apple.com/en-euro/108764>, accessed on 20 February 2025.

⁵⁵² Agreed minutes of meeting with [third-party developer] of 18 November 2024, paragraph 22.

5.10.2. *Feature falls within the scope of Article 6(7) of Regulation (EU) 2022/1925*

(520) The Commission finds that the automatic audio switching feature as described in Section 5.10.1 of this Decision falls within the scope of Article 6(7) of Regulation (EU) 2022/1925. Automatic audio switching is a feature which is controlled via iOS, Apple's operating systems for iPhones, which is listed in the Designation Decision.

5.10.3. *Current implementation for Apple's own services and hardware*

(521) Apple uses the information constituting the automatic audio switching feature as an input for its algorithm that operates on the audio-broadcasting devices and decides which audio source to play. Apps on iOS specify the relevant audio type (e.g. media, call, notification) when they start an audio session. Apple uses this category of information to infer priority for the purposes of automatic audio switching.⁵⁵³ Apple has a [...] policy among [...] its devices, as well as across first- and third-party apps, with regards to the order of priority of audio types for the purpose of automatic audio switching: [...].⁵⁵⁴ For audio routing, when Apple headphones (e.g. AirPods) are in use, which the iOS device can detect through the AirPods in-ear sensors, incoming calls are automatically routed to the AirPods, even when answered through the iPhone user interface.

5.10.4. *Current implementation for third-party services and hardware*

(522) Apple does not make the information constituting the automatic audio switching feature available to third parties.

(523) Apple submits that third parties can use Bluetooth Multipoint to achieve equivalent functionality to automatic audio switching.⁵⁵⁵ Bluetooth Multipoint is a configuration that allows a user to simultaneously connect an audio receiver, such as headphones, to more than one audio source device. However, as Bluetooth Multipoint maintains multiple Bluetooth connections in parallel (rather than switching between devices as available to Apple), it can lead to poor audio quality. Bluetooth Multipoint also lacks the necessary context, such as data on the type of audio being received, to intelligently prioritise audio between devices. It therefore relies on guesswork by the third-party audio receivers, and often leads to poor user experience.⁵⁵⁶

(524) Audio routing policies are different for third parties than for Apple. For third-party headphones, the behaviour depends on how the call is answered. If the call is answered through the buttons on the headphones (if available), the call is routed to the headphones. If instead the call is answered through the iPhone user interface, the call is routed to the iPhone speakers. Such different treatment of similar situations prevents effective audio switching for third parties even if they have access to contextual information, as incoming calls would not be routed to the third-party headphones.

(525) Therefore, the Commission considers that there is currently an interoperability gap when it comes to third-party connected physical devices connected to iOS devices and that it should specify how Apple has to fill this gap to comply with Article 6(7) of Regulation (EU) 2022/1925.

⁵⁵³ Apple's reply to RFI 3 of 7 October 2024, question 50.

⁵⁵⁴ Apple's reply to RFI 3 of 7 October 2024, question 50.

⁵⁵⁵ Technical meeting Apple/Commission of 3 October 2024, slide deck pages 31-32.

⁵⁵⁶ [Third-party developer]'s submission of 15 October 2024, pages 3-5.

5.10.5. *The gatekeeper's view*

- (526) Apple does not contest the measures relating to automatic audio switching in its reply to the Preliminary Findings. [...] ⁵⁵⁷
- (527) Concerning timing, Apple indicates that it is not able to introduce its solution by end of 2025. [...] ⁵⁵⁸
- (528) [...] ⁵⁵⁹
- (529) At a very late stage in the proceedings, Apple further submitted that it considers the functionality to present third-party connected physical devices which are not connected to the iOS device as a selectable audio route as outside of the scope of audio switching, and that it was not part of prior exchanges with the Commission. ⁵⁶⁰

5.10.6. *The Commission's assessment*

- (530) The Commission takes note that Apple's only feedback on the measures for automatic audio switching provided in its reply to the Preliminary Findings relate to the proposed timeline. [...]
- (531) In light of this, the Commission considers that [...] spring 2026, is acceptable.
- (532) Apple further indicates that the functionality to present non-connected third-party devices as available audio routes will take more time due to the need for standardisation. Apple indicated that it would provide more information concerning the necessary steps around standardisation, ⁵⁶¹ but has not done so during the proceedings.
- (533) The Commission considers that this functionality is necessary to allow effective interoperability with audio switching. Otherwise, third-party headphones would effectively be forced to maintain multiple active Bluetooth connections, which can affect audio quality (see recital (523) of this Decision). The shortcoming of maintaining multiple active Bluetooth connections was already set out in the Commission's Preliminary Findings, and not contested by Apple in its reply. ⁵⁶² Apple's position that the functionality to present non-connected third-party devices as available audio routes is not in scope of the audio switching feature, or that the necessity of this functionality had not been raised before, are therefore incorrect and must be rejected.
- (534) While standardisation is one route to make this functionality available to third parties, Apple also has the possibility to make its own protocol available to third parties. The Commission therefore considers that while additional time can be provided to make this functionality available, access to the functionality cannot be linked to a standardisation process. In particular, it is uncertain whether Apple will succeed to have this functionality included in the relevant Bluetooth standard, and so is the time required to do so. Furthermore, Apple has failed to provide details on how

⁵⁵⁷ Apple's reply to the Preliminary Findings, paragraphs 170-171.

⁵⁵⁸ Apple's reply to the Preliminary Findings, paragraph 172.

⁵⁵⁹ Email by Apple of 13 February 2025; Agreed minutes of meetings with Apple on 11 and 12 February 2025.

⁵⁶⁰ Email from Apple to the Commission on 20 February 2025 [on draft final measures].

⁵⁶¹ Email from Apple to the Commission on 13 February 2025 [on the draft final measures]; Agreed minutes of meetings with Apple on 11 and 12 February 2025.

⁵⁶² Preliminary Findings, paragraph 335.

standardisation would work, what the timeline would be, and even what the relevant standardisation body would be.

- (535) The Commission therefore considers that Apple should provide effective interoperability with the functionality to present non-connected third-party devices as available audio routes by spring 2027, i.e. at most one year after the expiry of the implementation deadline for the other audio switching functionalities.

5.10.7. Measures that Apple should implement

- (536) To meet the requirements of Article 6(7) of Regulation (EU) 2022/1925, Apple should implement an interoperability solution that provides third parties with access to the same automatic audio switching feature as available to Apple (as described in Section 5.10.1 of this Decision), in a way that is equally effective as the solution available to Apple.
- (537) This means that Apple should provide third parties access to the same data and information controlled or accessed by iOS that Apple uses to implement automatic audio switching functionality on Apple devices, and the ability to present their devices as a selectable audio route based on that information
- (538) Apple should not discriminate between its own and third-party connected physical devices in routing audio. Audio routing means iOS deciding and enabling to which output to route audio (e.g. in-built iPhone speaker, local speakers, wired or wireless headphones). Apple may allow users to set audio routing preferences, but must implement such user choice in a non-discriminatory manner.
- (539) For the purpose of audio routing, Apple should enable third parties to submit the same or similar device information to iOS and iOS must use that information in the same way as iOS uses the same or similar information from Apple connected physical devices (e.g. whether the headphone is in-ear).
- (540) Apple should make that data and information available to third parties at the same time as it is made available to the processes or services that implement the automatic audio switching functionality on Apple devices. For instance, this concerns changes in the data and information that Apple uses to implement automatic audio switching functionality on Apple devices.
- (541) Apple should grant third parties access to additional functionalities if necessary to enable effective interoperability with the automatic audio switching feature described in Section 5.10.1 of this Decision.
- (542) Apple should also provide effective interoperability with any future updates, including new functionalities, of the automatic audio switching feature insofar as they are available to Apple's own connected physical devices. To this end, the general measures in Section 5.12 of this Decision apply, including in particular the measures concerning future updates and new functionalities set out in Section 5.12.7 in this Decision.
- (543) Apple should implement the measures above in compliance with the measures for all features in Section 5.12 of this Decision.

5.10.8. Implementation timing

- (544) Apple should implement the measures for the audio switching feature by 1 June 2026 at the latest, with exception of the functionality to present non-connected third-party

devices as available audio routes. Apple should provide effective interoperability with that functionality by 1 June 2027 at the latest.

5.11. Measures for access to the NFC Controller in Reader/Writer Mode

- (545) NFC allows to exchange information between nearby devices that are up to a few centimetres apart. For years, iOS devices have implemented NFC technology, notably through the NFC controller, an iOS hardware feature. Apple uses NFC for many of its services and hardware. A prominent use case for the use of the NFC controller on iOS devices is Apple Pay: end users can add their payment cards to the Apple Wallet app via NFC (“Tap to Provision”⁵⁶³) and then use NFC technology of their iOS device to pay for goods in stores as they would do with a contactless payment card.
- (546) Third parties do not enjoy the same level of access to NFC. Apple does not allow third parties the use of NFC to automatically read a payment card’s details by bringing the card next to the iOS device. Similarly, companies offer connected physical devices, such as rings and watches, that contain an NFC chip and can be used to pay in the same way as contactless payment cards or Apple Pay on the iOS device. Such connected physical devices rely on the NFC controller of a smartphone to transmit payment credentials in the format of a token to the connected physical device – a process called provisioning of a token. The end user can simply use a smartphone app, which is generally developed by the provider of the connected physical device, to transmit the tokenised payment credentials by bringing the connected physical devices next to the smartphone.
- (547) Apple restricts access to the NFC controller for these use cases, while other operating systems allow full interoperability with the NFC controller in these instances.

5.11.1. Description of the feature

- (548) The NFC controller in Reader/Writer Mode feature consists of the ability of third parties to access and use the Reader/Writer mode of the NFC controller of iOS devices.
- (549) The NFC controller consists of a chip integrated in iOS devices, which enables communication between an iOS device and a connected physical device via NFC technology.⁵⁶⁴
- (550) NFC is a standardised wireless connectivity technology that allows the exchange of information if the communicating devices are within a range of a few centimetres.⁵⁶⁵ NFC has three modes of operation which define how NFC tags (i.e. small electronic

⁵⁶³ See <https://www.apple.com/newsroom/2024/06/new-features-come-to-apple-services-this-fall/>: “Additionally, with Tap to Provision, users can add eligible credit or debit cards to Apple Wallet by simply tapping their card to the back of their iPhone,” accessed on 15 November 2024.

⁵⁶⁴ Apple’s Proposal of Commitments to the European Commission, Case AT.40452 – Mobile Payments, https://ec.europa.eu/competition/antitrust/cases1/202428/AT_40452_10155330_9978_4.pdf, accessed 31 October 2024, paragraph 2.31 defines the NFC controller as a “chip integrated in an Eligible Device which includes an NFC frontend and a microcontroller capable of running application logic which ensures the communication between the device and the payment terminal through their antennas.”

⁵⁶⁵ Apple’s Proposal of Commitments to the European Commission, Case AT.40452 – Mobile Payments, https://ec.europa.eu/competition/antitrust/cases1/202428/AT_40452_10155330_9978_4.pdf, accessed on 31 October 2024, paragraph 2.30.

devices that store data, or devices, such as smartphones, that emulate one⁵⁶⁶) and NFC-capable devices can communicate with each other. The three modes are: (i) NFC Reader/Writer mode, (ii) NFC Peer-to-Peer mode, and (iii) NFC Host Card Emulation (HCE) mode.⁵⁶⁷ iOS devices support, and Apple uses, the Reader/Writer and HCE modes.⁵⁶⁸ The NFC Reader/Writer mode is the relevant mode for the examples of provisioning of a token to connected physical devices and reading payment cards (see recitals (545) and (546)).

- (551) NFC Reader/Writer mode is an NFC mode in which an active NFC device, such as an iOS device,⁵⁶⁹ interacts with a passive NFC tag.⁵⁷⁰ Passive NFC tags can, for instance, be integrated into connected physical devices, such as rings, watches or payment cards.⁵⁷¹ Apple has implemented third-party access to the NFC controller in Reader/Writer mode via *Core NFC*. *Core NFC* is a publicly documented framework that allows developers to program third-party apps that can access the NFC controller of iOS devices in Reader/Writer mode to write data to NFC tags, interact with protocol-specific tags, and read NFC tags.⁵⁷² As such, third-party apps can, for instance, transmit credentials in the format of a token via the NFC controller of the iOS device to connected physical devices (called “provisioning of a token”).⁵⁷³

5.11.2. Feature falls within the scope of Article 6(7) of Regulation (EU) 2022/1925

- (552) The Commission finds that the NFC controller in Reader/Writer mode feature as described in Section 5.11.1 of this Decision falls within the scope of Article 6(7) of Regulation (EU) 2022/1925. The NFC controller in Reader/Writer mode is a hardware feature that is controlled via iOS, Apple’s operating system for iPhones, which is listed in the Designation Decision.⁵⁷⁴

⁵⁶⁶ An NFC tag is a small electronic device that stores data and can wirelessly transmit that data to other NFC-enabled devices in close proximity without having an own power source. These tags are used for different purposes, such as information sharing, identity verification and contactless payments, see <https://www.idenfy.com/blog/what-is-an-nfc-tag/> accessed on 12 November 2024.

⁵⁶⁷ See <https://gototags.com/nfc/standards/modes>, accessed on 12 November 2024.

⁵⁶⁸ Apple’s reply to RFI 8 of 13 November 2024, question 1.

⁵⁶⁹ The “active” device is a device that device that is able to send and receive data, see <https://www.idenfy.com/blog/what-is-an-nfc-tag/> accessed on 12 November 2024.

⁵⁷⁰ See <https://gototags.com/nfc/standards/modes/reader-writer> accessed on 12 November 2024. The “passive” NFC tag is restricted to sending data since it does not have an own power source, see <https://www.idenfy.com/blog/what-is-an-nfc-tag/>, accessed on 12 November 2024.

⁵⁷¹ These passive NFC tags are NFC tags with a secure element that follow the ISO 7816 standard for so called “integrated circuit cards,” also called smart cards, see <https://www.iso.org/obp/ui/#iso:std:iso-iec:7816:-4:ed-4:v1:en>, accessed on 5 November 2024. In iOS, Core NFC provides the *NFCISO7816Tag* interface for interacting with such ISO 7816 tags, see <https://developer.apple.com/documentation/corenfc/nfciso7816tag>, accessed on 5 November 2024. It does so via a set of commands called Application Protocol Data Units (“APDUs”), see <https://developer.apple.com/documentation/corenfc/nfciso7816tag/3585173-sendcommand>, accessed on 5 November 2024.

⁵⁷² Since iOS 13 (released in 2019), Apple allows third parties to read and write NFC tags across multiple protocols: ISO 7816 and ISO 15693, FeliCa™, and MIFARE® tags and NFC tags of Types 1 to 5 that contain NDEF data. See Apple’s reply to RFI 2 of 30 September 2024, question 1 and Annex 1.2, point 1(vii); <https://developer.apple.com/documentation/corenfc/>, accessed on 15 November 2024; Apple’s internal document [...].

⁵⁷³ Apple’s reply to RFI 2 of 30 September 2024, question 1 and Annex 1.2, point 1(vii); [...].

⁵⁷⁴ Also see recital 56 of Regulation (EU) 2022/1925 that lists NFC technology as one example of technologies which can be required for the effective provision of a service provided by any potential third-party undertaking.

5.11.3. *Current implementation for Apple's own services and hardware*

- (553) Apple uses the NFC controller of iOS devices in Reader/Writer mode for NameDrop to share the user's contact information with other iOS devices and the Apple Watch, to add HomeKit devices to its Home App, to communicate with various Apple MagSafe accessories (e.g. AirTags, cases, wallets, batteries, and chargers) and for public APIs or Affordances.⁵⁷⁵
- (554) Furthermore, Apple uses the NFC controller of iOS devices in Reader/Writer mode (i) to accept⁵⁷⁶ contactless payments from NFC-enabled connected physical devices, including NFC-enabled payment cards, Apple Pay, Apple Watch, smartphones with other digital wallets, as well as (ii) to read loyalty and similar cards in Apple Wallet with "Tap to Pay"⁵⁷⁷ and (iii) to read physical transit cards for "Card ingestion."⁵⁷⁸ Apple announced the "Tap to Provision" feature in June 2024, which enables end users to add their payment cards to the Apple Wallet app via NFC by holding the card against the iPhone.⁵⁷⁹

5.11.4. *Current implementation for third-party services and hardware*

- (555) Apple provides third-party developers with Core NFC APIs.⁵⁸⁰ The Core NFC APIs provide access the NFC controller in order to interact with NFC tags, and in particular with ISO 7816 tags⁵⁸¹ that represent smart cards.⁵⁸²
- (556) By policy, Apple restricts third parties from using Core NFC APIs to access the NFC controller when using payment-related app identifiers ("AIDs") for ISO 7816 tags in Core NFC Reader/Writer mode, even though existing Core NFC APIs can perform this task.⁵⁸³
- (557) Connected physical devices that are used to perform payment transactions need to be provisioned with a token during their initial set-up. The token transferred in this case is a replacement of an actual payment card number.⁵⁸⁴ In order to launch the

⁵⁷⁵ Apple's reply to RFI 4 of 14 October 2024, question 41; Apple's reply to RFI 8 of 13 November 2024, question 4; Apple explains that the public APIs or affordances include the Mobile Document Reader in ProximityReader framework, the CoreNFC TagReader & NDEFReader and the Background Tag Reader & Universal Links.

⁵⁷⁶ Since iOS 13 (released in 2019), Apple allows third parties to read and write NFC tags across multiple protocols: ISO 7816 and ISO 15693, FeliCa™, and MIFARE® tags and NFC tags of Types 1 to 5 that contain NDEF data, see Apple's reply to RFI 2 of 30 September 2024, question 1 and Annex 1.2, point 1(vii). See as well <https://developer.apple.com/documentation/corenfc/>, accessed on 5 November 2024, and Apple's internal document [...].

⁵⁷⁷ Apple's reply to RFI 8 of 13 November 2024, question 4; and <https://developer.apple.com/tap-to-pay/>, accessed on 5 November 2024.

⁵⁷⁸ Apple's reply to RFI 4 of 14 October 2024, question 41 and Apple's reply to RFI 8 of 13 November 2024, question 4.

⁵⁷⁹ See <https://www.apple.com/newsroom/2024/06/new-features-come-to-apple-services-this-fall/>: "Additionally, with Tap to Provision, users can add eligible credit or debit cards to Apple Wallet by simply tapping their card to the back of their iPhone," accessed on 15 November 2024.

⁵⁸⁰ See <https://developer.apple.com/documentation/corenfc/>, accessed on 5 November 2024.

⁵⁸¹ See <https://developer.apple.com/documentation/corenfc/nfciso7816tag>, accessed on 5 November 2024.

⁵⁸² Apple's reply to RFI 8 of 13 November 2024, question 5.

⁵⁸³ Apple's reply to RFI 4 of 14 October 2024, question 44; see also the "Important" note on <https://developer.apple.com/documentation/corenfc/nfcstagreadersession>, accessed on 5 November 2024; [...].

⁵⁸⁴ Payment credentials take the form of a token (Device PAN), which is a proxy for the actual card number representation (Primary Funding PAN) generated upon end user request by the card provider,

provisioning of a token over NFC, which is particularly relevant for passive NFC-enabled wearables, the third-party app on the iOS device uses the NFC controller to connect to an app on the connected physical device. During this connection, the AID is revealed.⁵⁸⁵ Certain app identifiers are registered and therefore internationally unique,⁵⁸⁶ including the ones of payment apps, with for instance AIDs of apps for Visa and Mastercard.⁵⁸⁷ Apple blocks the use of the NFC controller in Reader/Writer mode via Core NFC when payment-related AIDs are used.⁵⁸⁸

- (558) Apple submits that it already provides effective interoperability for this use case. Apple submitted a link to a YouTube video from a third party that claims to have achieved the provisioning of payment credential tokens onto connected physical devices from an iPhone via an NFC connection.⁵⁸⁹ Apple admitted that it does not know how this third party achieved this result without detection by Apple’s app review mechanisms.
- (559) The Commission reached out to the third party to investigate how this third party managed to circumvent Apple’s payment-related AID restrictions in order to provision wearable devices with payment tokens.⁵⁹⁰ The technical solution implemented by this third-party constitutes a “workaround” as it relies on the use of a custom AID, different from the well-known registered payment AIDs.⁵⁹¹
- (560) The third party stated that the development of this process required several months of engineering work by multiple developers, and an adaptation of the firmware of the secure element chips to be integrated within the connected physical devices that involved negotiations over several months with and implementation by chip manufacturers. In addition, the solution currently only works seamlessly for payment cards issued by one payment scheme provider, which certified the third party, and with secure element chips developed by one chip manufacturer. To support another payment scheme to the same level, the same changes to the third-party app on the connected physical device would have to be made, including certification. Without the restrictions imposed by Apple, the third party asserts that it could have placed its product on the market several years earlier.⁵⁹²
- (561) Moreover, Apple could prevent the third party from continuing to use their technical solution, by blocking the “*install for personalization*” commands through iOS,

see technical meeting Apple/Commission of 24 October 2024, slide deck page 4; [third-party developer]’s submission of 27 August 2024, page 2.

585 The app issues an APDU command called ‘SELECT’ which contains the AID, see [third-party developer]’s submission of 27 August 2024, page 3; https://www.tfn.net/techno/smartcards/iso7816_4.html#ss9_3_2, accessed on 5 November 2024.

586 See <https://www.ansi.org/about/roles/registration-program/rid>, accessed on 5 November 2024.

587 See <https://www.eftlab.com/knowledge-base/complete-list-of-application-identifiers-aid>, <https://ambimat.com/developer-resources/list-of-application-identifiers-aid/>, <https://emv.cool/2020/12/23/Complete-list-of-application-identifiers-AID/>, all three accessed on 5 November 2024.

588 Apple’s reply to RFI 4 of 14 October 2024, question 44; see also the “Important” note on <https://developer.apple.com/documentation/corenfc/nfctagreadersession>, accessed on 5 November 2024.

589 Apple’s reply to RFI 4 of 14 October 2024, question 45.

590 Technical meeting Apple/Commission of 24 October 2024, slide deck page 12.

591 Agreed minutes of meeting with [third-party developer] of 29 October 2024, paragraphs 3 and 4.

592 Agreed minutes of meeting with [third-party developer] of 29 October 2024, paragraphs 5-7.

blocking the third party in accessing its Issuer Security Domain, or rejecting apps that rely on the solution during app review.⁵⁹³

- (562) The “workaround” implemented by the third party therefore does not constitute effective interoperability under Article 6(7) of Regulation (EU) 2022/1925.
- (563) Similarly to the process of provisioning a token to connected physical devices, several payment service providers and their trusted service managers established payment cards as a secure possession factor for strong customer authentication under the regulatory framework of Directive (EU) 2015/2366 (Payment Services Directive II).⁵⁹⁴ In order to verify this possession factor via an iOS device, iOS apps provided by payment service providers need to read the payment card. This process of verifying the possession factor via an iOS device could, for instance, replace the current practice of generating challenge/response codes through separate external bank card readers.
- (564) In order to do so, the payment service provider’s iOS app needs to communicate via the NFC controller of the iOS device in Reader/Writer mode with the Europay, MasterCard, and Visa (“EMV”) app on the payment card, which involves transmitting payment-related AIDs – the same way as laid out in recital (557) of this Decision for the process of provisioning a token, which is currently blocked on iOS. This process could provide iOS device users with a safer solution for customer authentication when performing banking related transactions, reducing the risk of phishing attacks. For example, social engineering is used to convince iOS device users to provide malicious actors with codes generated by the card reader, for instance via phone calls in which malicious actors pretend being bank employees. These malicious actors can then use the codes to set up the card on their own device and access the bank account of the respective iOS user to perform payment transactions, leading to financial losses for both, banks and their clients.⁵⁹⁵
- (565) Therefore, the Commission considers that there is currently an interoperability gap when it comes to third-party connected physical devices connected to iOS devices and that it should specify how Apple has to fill this gap to comply with Article 6(7) of Regulation (EU) 2022/1925.

5.11.5. *The gatekeeper’s view*

- (566) Apple considers that the measures in the Preliminary Findings are overly broad.⁵⁹⁶ In Apple’s view, the measures should (i) be limited to the specific use case of provisioning tokens to passive wearable devices,⁵⁹⁷ (ii) although Apple considers this would go beyond the scope of Article 6(7) of Regulation (EU) 2022/1925,⁵⁹⁸ and (iii) is not securely implementable within the timeframe specified by the Commission.⁵⁹⁹

⁵⁹³ Agreed minutes of meeting with [third-party developer] of 29 October 2024, paragraph 10.

⁵⁹⁴ Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

⁵⁹⁵ Agreed Minutes of meeting with [third-party developer] of 9 January 2025, paragraphs 1-3; [third-party developer]’s contribution to the public consultation.

⁵⁹⁶ Apple’s reply to the Preliminary Findings, paragraph 346.

⁵⁹⁷ Apple’s reply to the Preliminary Findings, paragraph 347.

⁵⁹⁸ Apple’s reply to the Preliminary Findings, paragraph 348.

⁵⁹⁹ Apple’s reply to the Preliminary Findings, paragraph 349.

- (567) *In the first place*, Apple argues that any specification in relation to the NFC controller in Reader/Writer Mode must be limited to the provisioning of tokens to passive wearable devices.⁶⁰⁰ *First*, Apple considers this being a matter of procedural fairness.⁶⁰¹ *Second*, Apple considers a use case-agnostic interoperability obligation as infeasible and inappropriate.⁶⁰² *Third*, Apple considers that use case-agnostic measures in relation to the NFC Controller in Reader/Writer mode feature would exceed what is available to Apple.⁶⁰³
- (568) In the second place, Apple argues that even the feature it refers to as “access to the NFC controller in Reader/Writer Mode for the provisioning of tokens to passive wearable devices” goes beyond the scope of Article 6(7) of Regulation (EU) 2022/1925.⁶⁰⁴ *First*, Apple considers that it is a feature not being used by Apple and argues that therefore the feature is not “available to” or “used by” an Apple service or hardware as required by Article 6(7) of Regulation (EU) 2022/1925.⁶⁰⁵ *Second*, Apple considers that it already provides for effective interoperability, since at least one developer uses NFC for provisioning tokens to passive wearable devices.⁶⁰⁶ *Third*, Apple considers that a use case-agnostic access to the NFC controller in Reader/Writer Mode is not necessary for its identified feature and outlines that different use cases present distinct integrity concerns and require tailored integrity measures while highlighting card skimming risks.⁶⁰⁷ Apple puts forward that the provisioning of tokens to passive wearable devices does not require the ability to transmit any application protocol data unit (“APDU”) command referencing AIDs or to read payment cards, which could in turn enable the use of the iPhone’s NFC controller to “skim” or access sensitive financial information and harm others. Apple argues that its current policy restrictions regarding payment-related AIDs are necessary and proportionate to prevent this. [...] ⁶⁰⁸
- (569) *In the third place*, Apple explains that it will not be possible for Apple to develop a solution that securely allows for the provisioning of tokens to passive wearable devices within three months of the notification of the final decision.⁶⁰⁹ [...] ⁶¹⁰

5.11.6. *The Commission’s assessment*

5.11.6.1. Concerning the scope of the NFC Controller in Reader/Writer mode feature not being limited to specific use cases

- (570) The Commission rejects the limitation of the NFC controller in Reader/Writer mode feature to the specific use case of provisioning tokens to passive wearable devices.
- (571) *First*, the Commission dismisses Apple’s allegations of maladministration. As outlined in Section 2.3 of this Decision, the Commission engaged with Apple extensively through technical meetings, calls and email exchanges aimed at assisting Apple in complying with its interoperability obligation under Article 6(7) of

⁶⁰⁰ Apple’s reply to the Preliminary Findings, paragraphs 350-361.

⁶⁰¹ Apple’s reply to the Preliminary Findings, paragraphs 351-355.

⁶⁰² Apple’s reply to the Preliminary Findings, paragraphs 356-360.

⁶⁰³ Apple’s reply to the Preliminary Findings, paragraph 361.

⁶⁰⁴ Apple’s reply to the Preliminary Findings, paragraphs 362-370.

⁶⁰⁵ Apple’s reply to the Preliminary Findings, paragraph 364.

⁶⁰⁶ Apple’s reply to the Preliminary Findings, paragraph 365.

⁶⁰⁷ Apple’s reply to the Preliminary Findings, paragraphs 366-370.

⁶⁰⁸ Email from Apple to the Commission on 2 February 2025.

⁶⁰⁹ Apple’s reply to the Preliminary Findings, paragraph 371.

⁶¹⁰ Email from Apple to the Commission on 2 February 2025.

Regulation (EU) 2022/1925. It is factually incorrect that the Commission did not mention the feature as being within the scope of this Decision in this context. The Commission did so on several occasions, both orally and in writing, and several Apple submissions confirm that Apple understood the scope of the feature correctly.⁶¹¹

- (572) *Second*, Apple itself explained that the NFC Reader/Writer mode is a single operation mode of the NFC controller,⁶¹² and the Commission does not consider it necessary to split it by introducing limitations to the use case of provisioning tokens to passive wearable devices.
- (573) *Third*, feedback received during the public consultation emphasized the relevance of having interoperability with this feature and confirmed that the proposed measures address relevant developers' requests while suggesting some clarifications.⁶¹³
- (574) *Fourth*, as outlined in Section 5.11.3 of this Decision, Apple uses the NFC controller in Reader/Writer mode feature for its own services and hardware. The Commission considers that it is not determinative for Apple's obligation to allow interoperability whether or not Apple offers a specific type of product or service, as set out in Section 3.1.4 of this Decision, since otherwise Apple could hamstring innovation by dictating which services or products can make use of the interoperability obligation, which would perpetuate its gatekeeping position, contrary to the objectives of Regulation (EU) 2022/1925.

5.11.6.2. Concerning the NFC Controller in Reader/Writer mode feature falling within the scope of Article 6(7) of Regulation (EU) 2022/1925

- (575) As outlined in Section 5.11.2 of this Decision, the Commission considers that access to the NFC controller in Reader/Writer Mode falls within the scope of Article 6(7) of Regulation (EU) 2022/1925. The provisioning of tokens to passive wearable devices is one possible use case that can benefit from interoperability with this feature. Apple uses this feature⁶¹⁴ and the possibility of a workaround for one third party does not establish effective interoperability and compliance with the obligation of Article 6(7) of Regulation (EU) 2022/1925.⁶¹⁵

⁶¹¹ As such, the Commission sent an email to Apple on 10 October 2024 with a set of questions on "NFC access for data transfer (read/write mode)" to guide the discussion of the technical meeting Apple/Commission of 24 October 2024 which covered the NFC controller in Reader/Writer Mode feature. [...] confirm that Apple understood the scope of the feature correctly. In line with this correct understanding, Apple refers in its follow-up submissions from 24 October 2024 / 6 November 2024 [...] and explains in a follow-up mail from 14 November 2024 that it considers [...]. In addition, the Commission's RFI 8 of 13 November 2024, included a question on the use by Apple of the NFC controller in Reader/Writer mode. The explanatory use case of reading of payment cards was explicitly mentioned during the courtesy call that took place on 21 November 2024. Finally, the Commission only obtained knowledge of the interoperability requests for interoperability with the NFC controller in Reader/Writer mode of [third-party developer] and [third-party developer], on 6 November 2024, when Apple sent its report to the Commission.

⁶¹² Apple's reply to the Preliminary Findings, paragraph 357.

⁶¹³ Contributions to the public consultation: contribution[s] from [third-party developers].

⁶¹⁴ See Section 5.11.3 of this Decision.

⁶¹⁵ See recital (558) to (562) of this Decision.

5.11.6.3. Concerning integrity

- (576) Regarding the integrity concerns brought forward by Apple, the Commission considers that Apple (i) errs in assuming that these could limit the scope of the interoperability obligation and (ii) fails to justify these.
- (577) *In the first place*, as outlined in Section 3.3 of this Decision, the burden is on Apple to duly justify the measures it intends to take to mitigate integrity risks as necessary and proportionate in the context of implementing effective interoperability. The integrity risks brought forward by Apple in relation to the NFC controller in Reader/Writer mode feature cannot put into question the obligation to allow effective interoperability for this feature. Apple confirmed that, as regards the feasibility of building an interoperability solution, i.e. technically opening up the feature, there are no integrity issues.⁶¹⁶ Any integrity issue should thus be limited to the implementation phase, i.e. possible adjustments under which that solution is made available to third parties.
- (578) *In the second place*, the Commission does not consider Apple's concerns relating to card skimming to fall under the integrity justification for the following reasons.
- (579) *First*, even though Apple referred on several occasions to card skimming risks through iOS devices via *Core NFC*, these references remained high-level and were not duly justified.⁶¹⁷ While Apple claims the existence of a card skimming risk in several instances, Apple fails to provide any specific evidence on this risk and its materialisation, for instance by providing data on card skimming that occurred using the NFC controller in Reader/Writer mode by third parties on other operating systems with the same or similar integrity risks, and hereby demonstrating the existence and magnitude of the integrity risk.⁶¹⁸ Apple also fails to outline how it addresses this risk for its own services and hardware that use the NFC controller in the Reader/Writer mode feature and why any differentiation in this regard for third-party services would be justified. Therefore, Apple's alleged integrity risks are nebulous and do not meet the standard of duly justifying its integrity concern, as required by Article 6(7) of Regulation (EU) 2022/1925.
- (580) *Second*, even if the alleged skimming risk was to exist, the skimming risk does not concern the integrity of iOS, or hardware or software features provided by Apple, as required by Article 6(7) of Regulation (EU) 2022/1925. Instead, it concerns a risk that an iOS device could be used as a tool to harm others (e.g. bank card holders in very close proximity). This is not a risk that threatens to impair the correct functioning of iOS, or hardware or software features provided by Apple. This use of the iOS device as a card skimming device is therefore not covered by the integrity clause of Article 6(7) of Regulation (EU) 2022/1925.

⁶¹⁶ Agreed minutes of meetings with Apple on 11 and 12 February 2025.

⁶¹⁷ Apple's submission of 14 November 2024 on [...]; Apple's statements during the technical meeting Apple/Commission of 24 October 2024 and accompanying slides [...]; Apple's reply to the Preliminary Findings, paragraphs 366-370; Apple's mark-up of the proposed measures of 23 January 2025, comments [A105, A106]; Email from Apple to the Commission on 2 February 2025.

⁶¹⁸ Considering for instance Apple's submission of 14 November 2024 [...] Apple explains that a restriction "*is necessary for security and privacy protection*," rather than integrity. Apple does not propose a concrete mitigating measure. [...] As well, it has been confirmed by [third-party developer] that no proof of abuse of access to the NFC controller has been reported for Android, which allows for access to the NFC controller since 2014, see agreed minutes of meeting with [third-party developer] of 29 October 2024, paragraph 11.

(581) *Third*, the Commission considers the card skimming risk via the NFC controller of an iOS device in Reader/Writer mode as remote, since NFC requires very close physical proximity, and any other NFC card reading capable device could potentially be used for card skimming. It is unclear why in particular iOS devices should be used for that purpose. Instead, the Commission considers that the reading of payment cards prevents iOS device users from harm and financial fraud caused by phishing attacks as submitted by payment service providers during the public consultation.⁶¹⁹ In addition, feedback received during the public consultation highlighted that third parties' security measures, such as EMV Level 2 kernels, could enhance iOS users' security, which is reflected in the measures Apple has to implement in the Annex to this Decision by clarifying that Apple should not restrict the deployment of these security measures when reading via the NFC controller in Reader/Writer mode smart cards.⁶²⁰

5.11.6.4. Concerning timing

- (582) While Apple argues that interoperability with the NFC controller in Reader/Writer mode feature is not securely implementable before spring 2026, the Commission considers that Apple does not propose any mitigating measures to its claimed integrity risks, besides the introduction of a warning prompt. The possible introduction of such a prompt does not alter the Commission's assessment regarding the implementation timeframe.
- (583) Apple has had a significant amount of time to consider and work on lifting interoperability restrictions for access to the NFC controller in Reader/Writer mode feature via *Core NFC*. Apple received the first formal requests for interoperability with the NFC controller in Reader/Writer mode via *Core NFC* in January 2024, which was analysed by Apple in June 2024.⁶²¹ At the same time, Apple has used for its own services and hardware most of the functionalities of the access to the NFC controller feature for several years, meaning that these functionalities are well established and known.
- (584) The Commission considers that the feature and the measures are of limited technical complexity, as the feature is already interoperable for other purposes.
- (585) End users already have the option to connect their iOS devices via NFC in Reader/Writer mode to connected physical devices. Currently, third parties can already use the *NFCISO7816Tag* protocol through Core NFC. Lifting current policy restrictions of Core NFC should therefore be achievable in a relatively short amount of time.
- (586) In order to accommodate Apple's development cycle though, the Commission adjusts the timeline as set out below under recital (595) of this Decision.

⁶¹⁹ [Third-party developer] contribution to the public consultation; agreed minutes of meeting with [third-party developer] on 9 January 2025, paragraphs 1-3.

⁶²⁰ [Third-party developer]'s contribution to the public consultation; this contribution as well as the updated Annex to this Decision, which includes the possibility of deploying third parties' security measures, such as EMV Level 2 kernels, have been submitted to Apple.

⁶²¹ Apple's internal document [...]. Apple analysed for instance the requests for interoperability with the NFC controller in Reader/Writer mode of [third-party developers] and categorised these requests [...].

5.11.7. Measures that Apple should implement

- (587) To meet the requirements of Article 6(7) of Regulation (EU) 2022/1925, Apple should implement an interoperability solution that provides third parties with access to the same NFC controller in Reader/Writer mode feature as available to Apple (as described in Section 5.11.1 of this Decision), in a way that is equally effective as the solution available to Apple.
- (588) The changes included in the measures that Apple should implement compared to the Preliminary Findings reflect the public consultation feedback.⁶²²
- (589) The NFC controller in Reader/Writer mode feature consists of all existing functionalities of the NFC controller while operating in Reader/Writer mode.
- (590) Such functionalities are:
- (a) interacting with NFC devices via the NFC controller in Reader/Writer mode through *Core NFC*, without restrictions on AIDs;
 - (b) transmitting any APDU command referencing AIDs, in particular payment-related AIDs, from a third-party app to a connected physical device through *Core NFC*, including the SELECT command, and any data that is part of the respective APDU command, including secure credentials;
 - (c) transferring secure credentials, including payment-related tokens, via the NFC controller of the iOS device to connected physical devices in Reader/Writer mode through *Core NFC*; and
 - (d) reading via the NFC controller in Reader/Writer mode smart cards, including payment cards, including to permit the verification of smart card possession through *Core NFC*, without restrictions on the deployment of third parties' security measures, such as EMV Level 2 kernels.
- (591) Apple should grant third parties access to additional functionalities if necessary to enable effective interoperability with the NFC controller in Reader/Writer mode feature described in Section 5.11.1 of this Decision.
- (592) Effective interoperability must be at least as effective as is available to any of Apple's services and/or hardware using access to the NFC controller in Reader/Writer mode, without the need for certifications and adaptations of features that are not required for Apple's services and/or hardware.
- (593) For the purpose of ensuring that effective interoperability continues in the future, third parties must also have access to any future updates, including new functionalities, of the NFC controller in Reader/Writer Mode feature insofar and as soon as they are available to Apple's services and/or hardware. For example, third parties should not be prevented from using future AIDs. To this end, the general measures in Section 5.12 of this Decision apply, including in particular the measures concerning future updates and new functionalities set out in Section 5.12.7 in this Decision.
- (594) Apple should implement the measures above in compliance with the measures for all features in Section 5.12 of this Decision.

⁶²² [Third-party developers'] contribution[s] to the public consultation.

5.11.8. *Implementation timing*

- (595) Apple should implement all measures to provide effective interoperability with the NFC controller in Reader/Writer mode feature through the use of Core NFC in the next major iOS release, i.e. iOS 19, and in any case by the end of 2025 at the latest.

5.12. **Measures for all features**

- (596) According to Article 6(7) of Regulation (EU) 2022/1925, interoperability provided pursuant to this provision needs to be effective. As described in Section 3.1.5 of this Decision, this means that interoperability solutions should be granted in a technically sound and workable manner for third parties, equally effective to the solutions available to Apple, under equal conditions, and without any undue obstacles. To achieve such effectiveness, the Commission considers it appropriate for Apple to implement certain measures for all of the features listed in Section 5 of this Decision.

5.12.1. *Integrity*

- (597) In line with Article 6(7) of Regulation (EU) 2022/1925, in the implementation of the specified measures, Apple may take strictly necessary and proportionate measures to ensure that interoperability does not compromise the integrity of the operating system, hardware and software features.⁶²³
- (598) In the context of these proceedings, Apple has not raised any integrity issues regarding the feasibility of building an effective interoperability solution in relation to the features listed in Section 5 of this Decision. Therefore, any integrity issues, if at all, will, in principle, be a matter of possible adjustments under which the interoperability solution will be made available to third parties pursuant to this Decision.⁶²⁴ The Commission also notes that Apple has not claimed nor substantiated any other obstacles which would constitute a barrier or make it impossible to develop an interoperability solution in relation to the features subject to this Decision.⁶²⁵
- (599) Under Article 6(7) of Regulation (EU) 2022/1925, and as explained in Section 3.3 of this Decision, any integrity measure shall be duly justified and based on transparent, objective, precise, and non-discriminatory conditions that also apply to Apple's services and hardware. Under the second subparagraph of Article 6(7) of Regulation (EU) 2022/1925, Apple should only impose conditions and take integrity measures that reflect a genuine integrity risk and do so in a consistent and systematic manner. Similarly, Apple should only apply conditions the compliance with which is capable of being independently verified and not exclusively within the gatekeeper's control. An integrity measure cannot be considered strictly necessary and proportionate if it seeks to achieve a higher integrity standard than the one that Apple requires or accepts in relation to its own services or hardware.⁶²⁶

⁶²³ See Article 6(7), second subparagraph of Regulation (EU) 2022/1925.

⁶²⁴ Apple confirmed that it was not aware of integrity concerns affecting the feasibility of building an interoperability solution as regards what Apple is currently working on based on today's knowledge and Apple cannot exclude that an issue could come up later. See agreed minutes of meetings with Apple on 11 and 12 February 2025, paragraphs 18 and 23.

⁶²⁵ Regarding Apple's claim that certain implementation deadlines are not technically feasible, see recital (684) of this Decision.

⁶²⁶ Apple claims in its reply to the Preliminary Findings, paragraph 85 that this requirement "*is misguided: granting third parties access to the same level of integration would inevitably create serious risks to the integrity and security of iOS and users' iPhones.*" The Commission notes that the requirement does not

- (600) The Commission also notes that it is important for the effectiveness in practice of the measures imposed by this Decision that no integrity measure is implemented in a way that would undermine effective compliance with this Decision and Apple's obligations with Regulation (EU) 2022/1925, including for instance by subverting end users' or business users' autonomy, decision-making, or free choice via the structure, design, function, or manner of operation of a user interface or apart thereof.
- (601) To ensure a proper monitoring of the effectiveness of the measures imposed by this Decision and to be in a position to assess the impact of any potential integrity measures on the effectiveness of the solutions ahead of their implementation, the Commission must put in place a reporting obligation. Such an obligation is necessary because integrity measures are not always easily observable but may have an impact on how third parties can benefit from the interoperability solution. Therefore, the Commission considers it necessary to be informed in writing of any integrity measure that Apple intends to take. In doing so, and in line with the requirements of Article 6(7) of Regulation (EU) 2022/1925, Apple should provide a relevant justification for the strict necessity and proportionality of the contemplated integrity measures. To prevent that interoperability solutions are further delayed, the information should reach the Commission at least four weeks in advance of the implementation of the integrity measures or without undue delay in case of urgency.
- (602) Nevertheless, some integrity measures are unlikely to significantly impact the effectiveness of the interoperability solution. As a result, the information obligation shall be limited in scope and Apple should not be required to inform the Commission of an integrity measure if it meets each of the following cumulative conditions: (i) it is not user-facing; (ii) it is exclusively of a technical nature; (iii) it is implemented for Apple and third parties in precisely the same way; and (iv) Apple has determined that the change will have no or only insignificant impact of any nature on third parties, including technical or commercial impact. Apple should retain written documentation on how any such determination was made.⁶²⁷

5.12.2. *Eligibility of beneficiaries, applications and use cases*

- (603) As outlined in Section 3.1.4 of this Decision, Article 6(7) of Regulation (EU) 2022/1925 does not provide for any limitations as to the beneficiaries, apps, products and use cases for interoperability with iOS hardware or software feature insofar as this feature is available to, or used by, Apple and intended to be used by a third party that is eligible under Article 1(2) of Regulation (EU) 2022/1925.
- (604) According to Apple, Article 6(7) of Regulation (EU) 2022/1925 only requires it to allow for effective interoperability vis-à-vis a third party that is a competitor of an Apple service or hardware in the Union.⁶²⁸

require that Apple grants all third parties the same level of integration, but merely that Apple must not impose a higher level of integrity than it applies to itself.

⁶²⁷ The Draft Final Measures shared with Apple on 7 February 2025 did not include this derogation. In an email sent to the Commission on 13 February 2025, Apple asked to restrict this reporting requirement to measures "with an impact exclusively in relation to third-party devices and not Apple's own connected devices," in order to avoid too frequent reporting. However, Apple's proposal would overly restrict the scope of the measures that Apple would report, notably because the same integrity measures may have a disparate impact on Apple's and third parties' services and hardware. The Commission considers that the derogation added to this Decision adequately addresses Apple's concerns without unduly limiting the scope of the reporting obligation.

⁶²⁸ Apple's reply to the Preliminary Findings, Sections I.B. and V.F.a.

- (605) As described in Sections 3.1.1 and 3.1.4 of this Decision, Apple’s interpretation is not supported by the language and aim of Article 6(7) of Regulation (EU) 2022/1925. Importantly, limiting interoperability to exactly those services and hardware that Apple offers would leave little room for innovation by third parties. In fact, it would always be Apple deciding which new services or hardware could be launched, effectively capping innovation at the level of Apple’s and only from the moment when Apple decides to launch the competing product. Instead, one of the key objectives of Regulation (EU) 2022/1925 is to foster and promote innovation in the digital sector and remove barriers that could prevent market participants from innovating.⁶²⁹ These objectives would be largely unattainable under Apple’s interpretation.
- (606) In the same vein, imposing restrictions on which apps can interoperate with a feature could significantly reduce the commercial incentives of third parties to invest and make use of the interoperability solution. An important example would be if third parties were prevented or discouraged from using the interoperability solution in their existing app distributed under its existing bundle ID,⁶³⁰ as this might force the third party to – *inter alia* – convince all end users in the Union or elsewhere to migrate to a different app.⁶³¹ Similarly, imposing restrictions on combining a feature with other features within the scope of Article 6(7) of Regulation (EU) 2022/1925 could significantly reduce the commercial incentives to make use of interoperability solutions.⁶³²
- (607) Therefore, the Commission considers it appropriate and necessary that Apple makes available the interoperability solutions and measures implemented in compliance with this Decision to all providers of services and of hardware without undue delay, to the extent they indicate, including through the use of APIs, an interest in making

⁶²⁹ See, for example, recitals 4, 32 and 107 of Regulation (EU) 2022/1925.

⁶³⁰ A bundle ID uniquely identifies an app in Apple’s App Store Connect (see <https://developer.apple.com/documentation/appstoreconnectapi/bundle-ids>, accessed on 12 February 2025). Requiring a new or separate bundle ID would force end users to download a different app in order to access the interoperability solution.

⁶³¹ [Association]’s contribution to the public consultation, Section 4.3.

⁶³² An example would be if third parties were prevented or discouraged from combining the use of the interoperability solution for the NFC controller in Reader/Writer mode feature with the use of the secure element feature, as this might force the third party to – *inter alia* – enter into a Payment Acceptance Platform agreement with Apple. See for instance contributions to the Public Consultation of [third-party developer]; [third-party developer]’s contribution to the public consultation, referring to the need to access the secure element, which is one of the explanatory features listed in recital 56 of Regulation (EU) 2022/1925. Another example would be the requirement for third parties to use *AccessorySetupKit* (see recital (263) of this Decision) in order to access some features, combined with a prohibition to use some functionalities of *Core Bluetooth*. Apple has confirmed to the Commission in a meeting on 3 February 2025 that they are considering requiring *AccessorySetupKit* for access to three features in this Decision: the iOS notifications feature, the automatic Wi-Fi connection feature, and parts of the background execution feature. However, during the respective tripartite meetings on 27 and 28 January 2025, [third-party developers] explained to the Commission and to Apple that some functionalities of *Core Bluetooth* – which they currently use – are currently prohibited by Apple for any app that uses *AccessorySetupKit*, and it is currently unclear whether *AccessorySetupKit* would provide an adequate alternative to enable the same functionalities. Therefore, if *AccessorySetupKit* remains incompatible with functionalities that are provided by *Core Bluetooth* but not by *AccessorySetupKit*, Apple’s implementation of the interoperability solution with these features should avoid any tying of *AccessorySetupKit* to those features. [...]

use of any or all of the features and/or functionalities in Section 5 of this Decision (hereinafter referred to as the “beneficiaries”).⁶³³

- (608) In the same vein and to ensure the effectiveness of the measures imposed in this Decision in practice, the Commission considers it appropriate to ensure that Apple does not limit the scope of this Decision through various restrictions on the use case pursued by the beneficiaries. Providing interoperability without restrictions as to the intended beneficiary, use case, or app reflects the language and aim of Article 6(7) of Regulation (EU) 2022/1925 and allows third parties to develop novel and innovative products that Apples does not yet offer.
- (609) In this context, Apple should not be allowed to impose any restrictions on the type or use case of the app and connected physical device that can access or make use of the features listed in Section 5 of this Decision. Similarly, Apple should not impose any undue restrictions, including by requiring third parties to use other Apple products or services unless required for the functioning of the feature, or by requesting third parties to make choices in situations where such choice is not justified (e.g. choosing between using the interoperability solution and continuing to use the same bundle ID⁶³⁴) or prevent third parties from benefitting from access to other features, including using the feature in combination with other features within the scope of Article 6(7) of Regulation (EU) 2022/1925.
- (610) If, under exceptional circumstances, Apple considers that the development or provision of an interoperability solution which is agnostic of the beneficiary, app or use case, may not be possible, Apple may, as described in Section 5.12.9 of this Decision, submit a reasoned request to waive this requirement.

5.12.3. *Equal effectiveness*

- (611) As outlined in Section 3.1.1 of this Decision, Article 6(7) of Regulation (EU) 2022/1925 requires that an interoperability solution offered to third parties must be equally effective and provided under equal conditions to the interoperability solution available to Apple’s own services and hardware.
- (612) According to Apple, Article 6(7) of Regulation (EU) 2022/1925 only requires an “effective” interoperability solution, which does not need to be “*equally effective*” to the solution available to Apple and does not need to be provided “*under equal conditions*” as the solution available to Apple’s services or hardware. In particular, Apple argues that there is no obligation to provide equality or parity of conditions. Similarly, Apple argues that there is no obligation to allow third-party services and hardware access to the same functionalities of the feature as are available to Apple under its interoperability solution.⁶³⁵
- (613) As explained in Section 3.1.1 of this Decision, Apple’s position is contradicted by the language and aim of Article 6(7) of Regulation (EU) 2022/1925 and its respective recitals. The provision refers to “*the same features*,” and the respective recitals highlight the need for interoperability which is “*equally effective*” to that available to the gatekeeper and offered “*under equal conditions*.” Apple’s interpretation of Article 6(7) of Regulation (EU) 2022/1925 would be contrary to the legislator’s aim

⁶³³ Beneficiaries may include third parties or app developers referenced in this Decision.

⁶³⁴ See recital (606) of this Decision.

⁶³⁵ Apple’s reply to the Preliminary Findings, Sections IV.A., IV.C. and V.C.

to ensure legal certainty and set out clear rules that can be directly applied so that business and end users can benefit from Regulation (EU) 2022/1925 without delay.

- (614) Therefore, the Commission considers it appropriate and necessary to ensure that Apple does not undermine effective interoperability with the features listed in Section 5 of this Decision by behaviour of a technical, commercial, contractual, or any other nature. Interoperability solutions should be granted in a manner that is technically sound, stable, and workable in practice for third parties without unnecessary hurdles.
- (615) In particular, the Commission considers it important for Apple to take certain measures which will ensure effective interoperability to be provided under equal conditions. Specifically, third parties should be in a position to make use of the interoperability solution in their existing apps via an automatic update of such apps. The Commission considers that this is an important requirement to ensure that the third parties' commercial incentives of using the interoperability solution are not affected. Indeed, since end user (re-)acquisition is generally expensive, providers of services and hardware typically prefer to add functionalities to their existing apps via an update that is automatically received by the end users who already have the app installed, rather than in a separate new app that end users must manually install.⁶³⁶ Having separate apps also creates fragmentation in the third party's offering, which adds complexity to development and end user acquisition.⁶³⁷ As explained in recital (606) of this Decision, the requirement to use a separate bundle ID is one of the ways in which third parties may be prevented from using the interoperability solution in their existing app. This measure is necessary to avoid such a restriction more generally, regardless of its causes.
- (616) Moreover, when end users choose to buy and use third-party services or hardware, such as smartwatches, they expect that such products will continue working as intended, with reliable and uninterrupted support for the functionalities that they provide to the end user. If the interoperability solution was designed or implemented by Apple, including via contractual terms, in a way that makes the third-party product unreliable for the end user, the user experience and the commercial value of the product could be substantially affected, as well as the third party's incentives to develop and bring that product to the market in the first place. For example, should an end user's smartwatch stop receiving iOS notifications as soon as the user temporarily travels outside of the EU – whereas the same does not happen for Apple Watch users – the user experience would be affected, putting the third-party smartwatch at a disadvantage. Therefore, Apple should not degrade, remove, disable, or otherwise make ineffective the interoperability solution, or prevent or impede updates, including security updates, for the end user as long as the end user is eligible to benefit from the functionalities allowed by these interoperability solutions under Regulation (EU) 2022/1925. Furthermore, should Apple decide to make the interoperability solution less effective once the end user is no longer eligible, it is important that the end user is duly informed, including to avoid that the end user mistakenly attributes the change in functionality to a malfunctioning of the third-party service or hardware. Therefore, before taking any such measure in this respect,

⁶³⁶ [Association]'s contribution to the public consultation, Section 4.3.

⁶³⁷ For example, user reviews on relevant app stores may be split across different apps. Moreover, the third party may need to provide multiple links to different apps on their website and advertising material, explaining to the user which links to use to install the right app.

Apple should notify the end user explaining how the measures Apple intends to take will affect the interoperability solution relied on by third-party services or hardware on the end user's iOS device.

- (617) Similarly, it is important that any interoperability solution implemented for the features listed in Section 5 of this Decision is equally effective to the solution available to Apple's own services and hardware, specifically Apple's own connected physical devices including, but not limited to, Apple Watch, AirPods, Apple Vision Pro, as well as any future Apple connected physical device. Such equal effectiveness applies across all dimensions, including, but not limited to, the end user journey, ease of use for end users, device and software setup, data transmission speed, and energy consumption.
- (618) Indeed, end user journey, ease of use, device and software setup, data transmission speed, and energy consumption all have an important impact on the user experience when using third-party services and hardware, and therefore on the commercial attractiveness of such services and hardware. The same is true for many other dimensions that have a direct or indirect effect on the user experience, such as default settings.⁶³⁸ If the interoperability solution for the features in scope of this Decision was not equally effective and under equal conditions as for Apple's services or hardware, including across these dimensions, third parties would be inherently disadvantaged. For example, if Apple were to implement the iOS notifications feature in a way which would delay the transmission of the notification to third-party connected physical devices compared to its own devices or require more battery use of the third-party connected physical device, the value proposition to end users by the third-party smartwatches would be negatively affected compared to the Apple Watch.
- (619) In particular, as explained in Section 3.1.5 of this Decision, the effectiveness of interoperability solutions could be undermined by introducing unnecessary "friction" when an end user uses third-party services or hardware. Friction has an impact on the ease, convenience, and speed of using the connected physical device and related apps from the end user perspective. Therefore, to ensure that the access to the features in scope of this Decision is equally effective to the solution available to Apple's services and hardware in terms of user experience, the Commission considers it appropriate and necessary to achieve effective compliance that Apple does not decrease the ease, convenience, and speed of using third-party services and hardware from the end user perspective, as compared to Apple's services and hardware.
- (620) To this end, the Commission considers that Apple should refrain from adding friction in the following ways.
- (a) Apple should not add friction by offering choices to, or requesting permission from, the end user in a non-neutral or leading manner, including by using design patterns, dark patterns, or misrepresenting or exaggerating any risks of using the third-party connected physical device (including related apps). An important example of techniques that exaggerate the risks are prompts that prominently inform the end user of risks based on the mere theoretical possibility that such risks might materialise. Especially if Apple were to

⁶³⁸ See e.g. Competition and Markets Authority, *Mobile ecosystems market study: Final report*, p. 265-270, <https://www.gov.uk/government/publications/mobile-ecosystems-market-study-final-report>, accessed on 24 February 2025.

exaggerate the risks only when using third-party services and hardware, the end user may simply conclude that third-party services and hardware are less safe than Apple's services and hardware – putting the former at an intrinsic disadvantage. Instead, Apple should inform the end user of any risk in a way that is neutral, appropriate to the likelihood that the risk may materialise, and non-discriminatory – also in compliance with the legal requirements on integrity measures, see Section 3.3 of this Decision.

- (b) Apple should not prevent the third party from explaining to end users in their own language the relevance of any system prompts shown, immediately before the prompt is shown or within the prompt. This allows the third party to provide more context to the end user as to why the system will show the prompt. For example, the companion app of the third-party connected physical device should be able to inform the end user of why access to a feature such as iOS notifications is needed to make the most out of the device, immediately before iOS shows the prompt to the user asking for their permission to grant such access to (the companion app of) the connected physical device.
- (c) Apple should not show unnecessary recurring prompts or notifications that the end user cannot easily and permanently disable in the same prompt or notification. Such recurring prompts or notifications can significantly affect user satisfaction for third-party services and hardware. While they may sometimes be appropriate to remind the end user of some choices or settings, the end user should always have the option to permanently disable them.
- (d) Apple should not prevent the third party from triggering a permission prompt again in the future, unless the end user has so decided. End users may not remember that they denied a third-party apps' requests for permission to access some feature (e.g. iOS notifications or Wi-Fi information) in the past. However, that permission may be necessary for the third party to provide a certain functionality to the end user. For this reason, the third party should be able to repeat the request to the user in the future, showing additional context that explains the request. In any case, the end user should have the option to prevent the repetition of that specific type of request from that specific third-party service or hardware.

5.12.4. *Free of charge*

- (621) Pursuant to Article 6(7) of Regulation (EU) 2022/1925, interoperability and/or access for the purposes of interoperability to hardware and software features accessed or controlled via the operating system as are available to services or hardware provided by the gatekeeper is to be provided free of charge. Apple shall not charge any fees, directly or indirectly, to beneficiaries for effective interoperability with the features within the scope of Article 6(7) of Regulation (EU) 2022/1925.
- (622) According to Apple, the “*free of charge*” obligation in Article 6(7) of Regulation (EU) 2022/1925 only applies to charge of access to overcome to a specific technical barrier for a third party to interconnect with a gatekeeper's hardware and software feature if this exists. Apple argues that this provision cannot preclude any indirect fees for any of the measures subject to this Decision, such as product validation.⁶³⁹

⁶³⁹ Apple's reply to the Preliminary Findings, Section V.F.c.

- (623) As described in Section 3.1.1 of this Decision, Article 6(7) of Regulation (EU) 2022/1925 is a results-based obligation with the goal of enabling effective interoperability. In line with this goal, this Decision requires Apple to implement the measures required by third-party services and hardware to access or interoperate with some specific iOS features. Therefore, all implementation steps to enable that the desired result of interoperability can be achieved in practice fall within the scope of Article 6(7) of Regulation (EU) 2022/1925 and have to be provided free of charge. It is also entirely unclear where Apple would want to draw the line between measures needed to “*overcome a specific technical barrier*” and other measures. Apple itself does not identify any specific measure listed in the Preliminary Findings which it would want to charge for, except for a vague reference to “*product validation*”. [...] ⁶⁴⁰ [T]he Commission takes position in this Decision that to the extent Apple puts in place such a process to implement its obligations under Article 6(7) of Regulation (EU) 2022/1925, this process should be free of charge as prescribed in the article at stake.
- (624) Therefore, the Commission considers that to comply with the requirements of Article 6(7) of Regulation (EU) 2022/1925, interoperability solutions implemented to address the measures listed in Sections 1 to 9 of the Annex to this Decision should be free of charge, irrespective of their beneficiary, app, product and use case. Apple should also not charge any fees directly or indirectly for any of the measures set out in the Annex to this Decision.

5.12.5. Documentation, frameworks, and APIs

- (625) As described in Section 3.1.5 of this Decision, Article 6(7) of Regulation (EU) 2022/1925 requires an interoperability solution to be effective. This means that the interoperability solution must work in practice and be “fit for purpose” and accessible to third parties.
- (626) According to Apple, the requirement described in the Preliminary Findings to make available and maintain complete, accurate, and well-documented frameworks and APIs – to the extent that access to those is relevant for the implementation of the measures subject to these proceedings – is unnecessary to allow effective interoperability and ignores Apple’s IPRs, in particular the protection of Apple’s copyrights, trade secrets, and patents. ⁶⁴¹
- (627) In this context the Commission notes that, generally, Apple enables interoperability with iOS features through access to its SDKs, through which the relevant frameworks and APIs are provided (see recital (132) of this Decision). Frameworks and APIs are typically accompanied by proper documentation, so that they can effectively be used by the developers. Such documentation is usually critical for third parties to build apps in practice, as it contains all the information required to make use of the frameworks and APIs in third-party apps, with details about the classes, methods, return types, arguments and more, often supported by tutorials and examples. Apple did not provide any specific arguments as to why, in the context of the current proceedings, such information would not be necessary for developers to allow effective interoperability. Therefore, the Commission considers that Apple should not depart from its practice of adequately documenting its interoperability solutions in the context of these proceedings.

⁶⁴⁰ Apple’s reply to the Preliminary Findings, paragraphs 316-317.

⁶⁴¹ Apple’s reply to the Preliminary Findings, Section V.F.e.

- (628) Moreover, as explained in recital (79) of this Decision, the Commission considers that making available and maintaining complete, accurate, and well-documented frameworks and APIs is necessary to enable developers to understand and effectively use the interoperability solution. Such an obligation is therefore an unavoidable corollary of allowing effective interoperability with iOS features pursuant to Article 6(7) of Regulation (EU) 2022/1925. As such, it does not disproportionately interfere with Apple's right to property under Article 17 of the Charter.
- (629) Therefore, the Commission considers is proportionate and appropriate to oblige Apple to provide complete documentation of all interoperability solutions it will be making available in compliance with this Decision. This includes Apple making available complete, accurate, and well-documented frameworks and APIs to the extent access to such frameworks or APIs are relevant for the implementation of the measures set out in this Decision.

5.12.6. *Assistance and testing*

- (630) For interoperability solutions to be effective and workable in practice, third parties must be able to receive adequate technical assistance for the purpose of implementing effective interoperability in relation to the features within the scope of this Decision. In addition, interoperability solutions must be sufficiently tested, in line with Apple's usual testing cycles and practices.
- (631) According to Apple, Article 6(7) of Regulation (EU) 2022/1925 does not require it to provide unlimited technical support to third parties. Apple argues that such an obligation would allow third parties to profit free of charge from its innovations and investment and divert Apple's resources.⁶⁴²
- (632) The Commission considers that while Apple does not need to provide unlimited technical support to third parties, Apple is required to provide the support and testing that is required so that third-party services and hardware can interoperate with the features subject to this Decision as effectively as Apple's services and hardware can. This follows from two related principles of Article 6(7) of Regulation (EU) 2022/1925. First, the obligation is results-oriented and third parties need to be in a position to be able to effectively interoperate with the respective feature. Second, the interoperability solution needs to be equally effective to that available to Apple. Therefore, to the extent third parties require reasonable technical assistance to achieve such interoperability, the Commission considers that it falls within the scope of Article 6(7) of Regulation (EU) 2022/1925 and needs to be provided by Apple, free of charge.
- (633) Similarly, to achieve results-oriented and effective interoperability, all interoperability solutions implemented to address the measures specified in this Decision need to be subject to Apple's usual practices, including beta testing. Testing is crucial for Apple to develop a functioning interoperability solution and for developers to familiarise themselves with that interoperability solution and identify its scope, possibilities, and importantly its shortcomings and issues. Beta testing is an opportunity for end users and business users who opted to receive beta updates to test the interoperability solution to uncover any bugs or issues in the interoperability solution (or in its use by the third-party service or hardware) before its general release.

⁶⁴² Apple's reply to the Preliminary Findings, Section V.F.f.

- (634) Therefore, the Commission considers it appropriate and proportionate in the context of these proceedings to oblige Apple to provide reasonable technical assistance, and to follow its usual practices including beta testing to the benefit of business users implementing effective interoperability with the features subject to this Decision.

5.12.7. *Future updates and new functionalities*

- (635) As outlined in Section 3.1.3 of this Decision, Article 6(7) of Regulation (EU) 2022/1925 aims to ensure that third-party providers of services and hardware relying on an operating system are able to provide their services and hardware on a level playing field with the gatekeeper's services and hardware as regards access to operating system features.⁶⁴³ It is therefore crucial that third-party providers of connected physical devices obtain effective access to any updates of new functionalities of features subject to this Decision, at the same time and under the same conditions as Apple. In practice, this means that third parties need to be able to test any of such planned updates or new functionalities and obtain access to them once they are available to Apple's own services or products.
- (636) According to Apple, an obligation to allow interoperability for future updates, including new functionalities, of the features controlled or accessed by iOS at the same time as they are available to Apple is not within the scope of Article 6(7) of Regulation (EU) 2022/1925 and would limit Apple's incentives to innovate, increase the development cost of new features, reduce Apple's competitive advantage, and allow third parties to free ride on Apple's innovation.⁶⁴⁴
- (637) As described in Section 3.1.3 of this Decision, Article 6(7) of Regulation (EU) 2022/1925 stipulates a simple rule: if a feature is available to or used by Apple, it needs to be made fully available and fully interoperable for third parties. Providing interoperability with new features and functionalities does not deprive Apple of its incentives to innovate or of any competitive advantage.⁶⁴⁵ Apple will continue to benefit from its innovation on iOS and its own services and hardware. As the developer of iOS, Apple manages the prioritisation of feature development as well as the timing, allowing Apple to focus on new features that will be used by its own services or hardware. Moreover, Apple is the only one to know which iOS features are currently being planned and developed and can use this knowledge for the development of its services and hardware which make use of the respective iOS features, with an unavoidable head-start compared to the market. The Commission notes in this context that, contrary to what Apple claims, neither Article 6(7) of Regulation (EU) 2022/1925 nor this Decision require Apple to disclose its internal development plans and pipeline to third parties.
- (638) Therefore, the Commission considers it proportionate and appropriate to achieve the goals of contestability and fairness that Apple, should it make changes to a feature listed in this Decision, including adding new functionalities to the feature or making updates, should: (i) develop such new or updated features or functionalities in a way that they are interoperable with third-party services or hardware; (ii) include the interoperability solutions at an appropriate time in the beta version of the new or updated feature or functionality; and (iii) make available the updated interoperability

⁶⁴³ Recital 55 of Regulation (EU) 2022/1925.

⁶⁴⁴ Apple's reply to the Preliminary Findings, Sections F.D. and V.F.d.

⁶⁴⁵ See also Section 3.2 of this Decision.

solution and documentation for the relevant feature no later than at the time the new or updated feature becomes available to any Apple's services or hardware.

- (639) After releasing an interoperability solution that provides a certain feature, Apple should ensure that the interoperability solution remains effective over time. This includes any maintenance⁶⁴⁶ tasks required to ensure the continued availability, correct functioning, and usability of the interoperability solution and, where applicable, its documentation, for all developers. Such tasks include making the necessary changes to preserve compatibility with newer iOS versions and extending changes in documentation style or structure to the interoperability solutions.
- (640) Over time, certain software and hardware capabilities may become obsolete, go out of fashion, or be superseded by better alternatives, including in response to improvements in integrity standards or the discovery of vulnerabilities. In such cases, the gatekeeper may decide, subject to the requirements of Article 6(7) of Regulation (EU) 2022/1925, to adjust or deprecate (parts of) an interoperability solution that it provides to third parties. When deciding on the deprecation of interoperability solutions, the gatekeeper should refrain from taking deprecation decisions that could constitute a circumvention of Article 6(7) of Regulation (EU) 2022/1925 in the meaning of Article 13 of Regulation (EU) 2022/1925, such as degrading the conditions or quality of iOS as provided to third parties who avail themselves of the rights laid down in Article 6(7) of Regulation (EU) 2022/1925.
- (641) Effective interoperability requires that third-party developers can rely on the interoperability solution over time. Third parties develop their hardware and services based on the interoperability solution and make significant investments for this purpose. A deprecation or discontinuation of an interoperability solution could significantly impact the functioning of third-party services and hardware and therefore the developer's investments, and ultimately the incentive to start and continue innovating based on iOS interoperability solutions. Third parties cannot be obliged to adapt their implementation at short notice or lose interoperability, as they depend on these interoperability solutions for their services and hardware. In particular in the case of hardware, products that are already in development or have been sold to consumers are built with the assumption that the hardware and software features of the operating system necessary for their functioning will remain available.
- (642) Third parties have repeatedly requested effective interoperability with the features listed in this Decision,⁶⁴⁷ proving significant market demand. Moreover, the market of connected physical devices is expected to continue growing for an extensive period of time.⁶⁴⁸ Deprecation of interoperability solutions for any of the features listed in this Decision would therefore cause substantial harm to third parties' ability to provide existing and new services and hardware for connected physical devices. The risk of deprecation in the future would also diminish the third parties' incentives to make the substantial investments that may be necessary for innovation and

⁶⁴⁶ Wherever measures in this section address maintenance or adjustment of an interoperability solution, this maintenance or adjustment covers, among others, any software changes concerning the interoperability solution. This is agnostic to the choice of how such changes are made, such as, by "refactoring" (i.e. restructuring) the existing code. This may include the creation of (and replacement by) a new framework, in the case where this is the most appropriate way of maintaining or adjusting the interoperability solution.

⁶⁴⁷ See recital (121) of this Decision.

⁶⁴⁸ See recital (12) of this Decision.

contestability of Apple's services and hardware. The Commission therefore considers it proportionate and appropriate that the interoperability solutions for the well-defined set of features listed in this Decision are preserved over time without interruption. If, in exceptional circumstances, Apple, in the context of its operations, considers it necessary to deprecate an interoperability solution or parts of it for any of the features listed in this Decision, Apple may submit a reasoned request in accordance with the procedure described in Section 5.12.9 of this Decision.

5.12.8. *Reporting*

- (643) Pursuant to Article 26 of Regulation (EU) 2022/1925, the Commission shall monitor gatekeepers' compliance with a decision adopted pursuant to Article 8(2) of that Regulation.
- (644) To this end, in the context of the case at hand, the Commission considers it important for Apple to report to the Commission the details of its implementation plans concerning the specified measures. To allow for the identification and resolution of any potential shortcomings or issues in the context of a constructive dialogue between the Commission and Apple, potentially involving the third parties as relevant, Apple should report shortly after the notification of the Decision.
- (645) Under this reporting obligation, Apple should also report on the actual interoperability solution once the solution has been implemented. To allow for a proper assessment of the implemented interoperability solutions, the Commission might need to consult third parties. For this purpose, Apple must prepare a non-confidential version of its implementation report. In its reporting, Apple must also outline, to the extent applicable, any measures it intends to take or has taken, to ensure the integrity of iOS when implementing the measures specified in this Decision.
- (646) In the context of its response to the Preliminary Findings, Apple argues that the reporting obligation finds no support in the text, context, or purpose of Article 6(7) of Regulation (EU) 2022/1925. Regulation (EU) 2022/1925 provides for two reporting obligations only – in Article 11 of that Regulation for the compliance report and in Article 26 of that Regulation for the monitoring of obligations and measures. In particular, Apple argues that the reporting obligation prior to the implementation of the specified measures above goes beyond what is necessary to monitor compliance within the remit of Article 26 of Regulation (EU) 2022/1925.⁶⁴⁹
- (647) As outlined in recital (643) of this Decision, Article 26 of Regulation (EU) 2022/1925 empowers the Commission to take the necessary actions to monitor the gatekeeper's effective implementation and compliance with a decision taken pursuant to Article 8(2) of that Regulation. A timely and effective implementation of the measures specified in this Decision is key to meet the objectives of Article 6(7) of Regulation (EU) 2022/1925 of effective interoperability and ultimately contestability. To ensure a timely and effective implementation, it is necessary that the Commission understands how Apple plans to implement the respective interoperability solutions. Only a reporting before the actual implementation will allow for the identification and resolution of potential shortcomings or issues in the context of a constructive dialogue between the Commission and Apple.

⁶⁴⁹ Apple's reply to the Preliminary Findings, Section V.F.g.

- (648) Therefore, the Commission considers it appropriate and proportionate for Apple to communicate to the Commission within one month of the date of notification of this Decision all the measures that it intends to take to comply with the Decision in sufficient detail to enable the Commission. In particular, Apple should: (i) describe in detail the interoperability solution it intends to make available; (ii) explain how this solution addresses all of the measures in the Decision and will provide third parties effective interoperability under equal conditions to those available to Apple's services and hardware; and (iii) provide detailed planning of the steps leading to the implementation and release of the effective interoperability solution.
- (649) Once Apple has implemented an interoperability solution for a feature subject to this Decision, the Commission considers it necessary and proportionate for Apple to communicate the measures that it has taken to comply with this Decision, so that the Commission can carry out its monitoring obligations. Specifically, to enable the Commission to review and monitor Apple's interoperability solution, Apple should describe the interoperability solution made available to third parties, including all technical details and potential APIs, as well as any potential integrity measures. To enable third parties to review, consult, and comment on the interoperability solution, it is important that Apple provides the Commission with a non-confidential version of this report for publication.

5.12.9. *Waiver*

- (650) Given the technical complexity associated with the implementation of the measures in the Annex to this Decision, it cannot be excluded that, in exceptional circumstances, for legal, technical, or other reasons, Apple may not be in a position to implement one or more of the measures or a part of them. In such cases, the Commission may, in response to a reasoned request from Apple showing good cause, modify or substitute one or more of the measures or a part of them. To ensure the effectiveness and timely implementation of the measures, it is important that the request does not have the effect of suspending the implementation of the measures and, in particular, of suspending the expiry of any time period in which the measure has to be complied with.

6. PROPORTIONALITY

- (651) Pursuant to Article 8(7) of Regulation (EU) 2022/1925, in specifying the measures that the gatekeeper concerned is to implement in order to effectively comply with its obligations, the Commission shall ensure that the measures are effective in achieving the objectives of that Regulation and the relevant obligation, and that they are proportionate in the specific circumstances of the gatekeeper and the relevant service. Subject to the principle of proportionality, limitations on the exercise of the rights and freedoms recognised by the Charter may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.⁶⁵⁰
- (652) Apple argued in its response to the Preliminary Findings that the measures disproportionately interfere with Apple's rights under Article 17 of the Charter and that Apple's right to conduct its business and compete on privacy and security grounds is protected by Article 16 of the Charter of Fundamental Rights.

⁶⁵⁰ Article 52(1) of the Charter.

6.1. Right to property

- (653) Apple argued that the measures in this Decision would disproportionately interfere with Apple's IPRs under Article 17 of the Charter. In doing so, Apple referred to its explanation in its response to the Preliminary Findings in case DMA.100204 to support that the requirement to disclose information on its proprietary technologies would disproportionately interfere with its IPR.⁶⁵¹ The measures would even further interfere with Apple's IPR by requiring Apple to provide third parties with access to its proprietary software implementations, to allow third parties to copy these implementations, and to use Apple's patented technology in the process.⁶⁵² Apple further submitted that the Preliminary Findings neither acknowledge Apple's fundamental rights nor contain a proper assessment of proportionality.⁶⁵³ Specifically, Apple claims that requiring interoperability with AirPlay would interfere disproportionately with its fundamental rights and invokes IPRs, including copyright.⁶⁵⁴ In addition, Apple submits that the obligation to provide documentation ignores Apple's IPRs.⁶⁵⁵ The free-of-charge condition must be interpreted as narrowly as possible given the impact of the measures on fundamental rights (in particular property rights) and the principle of proportionality.⁶⁵⁶
- (654) Article 17 of the Charter and Article 1 of the First Protocol to the European Court of Human Rights grant everyone the right to own, use, and dispose of their lawfully acquired or created property, including their intellectual property, to the exclusion of third parties.
- (655) The Commission notes that Apple is best placed to substantiate which IPR protected in the Union it holds, and which would be interfered with by the draft measures. However, Apple did not adequately substantiate its claim that compliance with these measures would interfere with Apple's IPR protected in the Union.
- (656) During the administrative proceedings, including in its Response to the Preliminary Findings, Apple only named concrete IPR with respect to two features. [...] each in a bullet on a slide presented during a meeting on 18 October 2024.⁶⁵⁷ Apple did not provide any further information in relation to the alleged IPR. Based on the Commission's research, only "US20180091923A1" appears to be a valid U.S. patent number; publicly available information provides that this number refers to an "application [which] claims the benefit of priority of U.S. Provisional Patent Application No. 62/399,250, filed Sep. 23, 2016."⁶⁵⁸ Importantly, none of the above features were included in the Preliminary Findings or in this Decision.
- (657) The only other mentions of IPRs are contained in footnotes in Apple's submissions in relation to the various features in which Apple merely reserves its right with respect to the legal interpretation and its legal position including regarding

⁶⁵¹ Apple's reply to Preliminary Findings, in particular paragraphs 19-22, 107, referring to Apple's reply to Preliminary Findings on Process (DMA.100204), in particular Sections IV, V.

⁶⁵² Apple's reply to Preliminary Findings, paragraphs 5, 19-22, 61, 103, 112-116.

⁶⁵³ Apple's reply to Preliminary Findings, paragraphs 103, 117, 375.

⁶⁵⁴ Apple's reply to Preliminary Findings, paragraphs 8, 247.

⁶⁵⁵ Apple's reply to Preliminary Findings, paragraphs 103-104, 107.

⁶⁵⁶ Apple's reply to Preliminary Findings, paragraphs 39, 98.

⁶⁵⁷ Technical meeting Apple/Commission of 18 October 2024, slide deck pages 6, 7, and 9.

⁶⁵⁸ Based on the European Patent Office's web search, <https://worldwide.espacenet.com/>.

fundamental rights, proportionality, and its relevant IP rights.⁶⁵⁹ However, the submissions themselves do not discuss fundamental rights or IPR, except for a short letter which, without substantiating the IPR at issue, calls for a balancing exercise taking account of restrictions of Apple’s freedom to do business and right to property, Apple’s freedom to differentiate its products in competition, Apple’s incentives to innovate, privacy, security, consumer interests, complexity and extent of engineering effort, and intrusion on Apple’s IP and other rights.⁶⁶⁰ Apple included a similar footnote in its responses to the Commission’s RFIs. Apple claims that it raised in four RFI responses that the measures would disproportionately interfere with its IPR.⁶⁶¹

- (658) The Commission considers that in no case did Apple adequately substantiate its generic claims or provide the Commission with sufficient information to assess its claims. *First*, two points referred to in Apple’s reply to the Preliminary Findings⁶⁶² concern Apple’s claims with respect to AirDrop and AirPlay, two features which are not within the scope of this Decision.⁶⁶³ *Second*, another point⁶⁶⁴ concerns Apple’s claim that making AWDL available to third parties would interfere with Apple’s IPRs. This Decision does not, however, require interoperability with AWDL regarding the P2P Wi-Fi connection feature. *Third*, another point⁶⁶⁵ concerns Apple’s opposition to a question in an RFI requesting Apple’s internal documentation of private APIs for certain features (some of which are covered by this Decision), which Apple claims is protected by trade secrets.⁶⁶⁶ Apple’s claim is thus solely about internal documentation and limited to the documentation requested in the RFI. Apple does not explain how their claims apply to the measures in the Preliminary Findings or the Draft Final Measures. In any case, Apple’s claim of an alleged loss of the commercial value behind the technology and threat to Apple’s business interests is unsubstantiated.
- (659) Equally unsubstantiated are Apple’s references to two further RFI responses in footnotes to its Response to the Preliminary Findings.⁶⁶⁷ One RFI response contains one paragraph where Apple states that all of its APIs are protected by trade secrets and other IPR.⁶⁶⁸ It is unclear what Apple is referring to in the other RFI response, possibly that certain information is only available “on a need-to-know” basis within Apple.⁶⁶⁹

⁶⁵⁹ See Apple’s submission of 15 November 2024 [...], footnote 1; Apple’s submission of 24 October 2024 [...], footnote 1; Apple’s submission of 6 November 2024 [...], footnote 1; Apple’s [submission] of 14 November 2024, footnote 1; Apple’s submission of 14 November 2024 [...], footnote 1; Apple’s submission of 7 November 2024 [...], footnote 1.

⁶⁶⁰ Apple’s letter to the Commission of 15 October 2024, paragraph 15.

⁶⁶¹ Apple’s reply to Preliminary Findings, paragraph 114.

⁶⁶² Apple’s reply to Preliminary Findings, paragraph 114, lit b. and d.

⁶⁶³ These features were included in the Preliminary Findings, but not in this Decision. This Decision does not take a position whether, and under what circumstances, Apple must allow interoperability under Article 6(7) of Regulation (EU) 2022/1925 with AirPlay and/or AirDrop.

⁶⁶⁴ Apple’s reply to Preliminary Findings, lit c.

⁶⁶⁵ Apple’s reply to Preliminary Findings, lit a.

⁶⁶⁶ Apple’s reply to RFI 2 of 30 September 2024, question 1.b.

⁶⁶⁷ Apple’s reply to Preliminary Findings, footnotes 74 and 364.

⁶⁶⁸ Apple’s reply to RFI 3 of 7 October 2024, question 4.

⁶⁶⁹ Apple’s reply to the request for input of 14 October 2024, page 10. Apple claim that it raised concerns about the impact on its IPR during two technical meetings (see Apple’s reply to Preliminary Findings, footnote 365 and paragraph 374) is equally unsubstantiated.

- (660) Apple has also not substantiated its claim that any interference by this Decision with its IPR would be disproportionate. In particular, Apple has not explained why the interference with its IPR by this Decision is of such nature and weight to cast aside, in this particular case, the Union legislator's weighing of the public interests against the private interests of economic operators impacted by that legislation as reflected in the wording of Article 6(7) of Regulation (EU) 2022/1925, which does not provide for a justification based on IPR.
- (661) The Commission cannot assess Apple's claim that the free-of-charge condition must be interpreted as narrowly as possible to prevent a disproportionate interference with Apple's IPR, because Apple has not substantiated the existence of a protected IPR or any interference therewith in relation to any of the features subject to this Decision.
- (662) Similarly, Apple did not substantiate its claim that the obligation to provide documentation ignores Apple's IPRs. It is insufficient to refer to "*Apple's IPRs, in particular the protection of Apple's copyrights, trade secrets.*"⁶⁷⁰ In addition, to the extent Apple develops an interoperability solution for third parties while using a different solution for its own services and hardware, Apple does not have to document APIs of its internal solution.⁶⁷¹
- (663) Finally, as concerns Apple's claim that the Commission should have engaged with its claims in its Preliminary Findings, the Commission notes that due to the lack of substantiation of Apple's claims regarding IPR, the Commission was neither able nor obliged to assess them in the Preliminary Findings.
- (664) At a very late stage in the proceedings, Apple submitted a letter setting out its concerns that the specification proceedings interfere disproportionately with its IPRs. [...] ⁶⁷²
- (665) Apple's letter does not change the Commission's assessment.
- (666) *First*, the letter came too late in the proceedings to afford the Commission sufficient time to properly take it into account. The letter was submitted only four working days before the legal deadline and one working day before the scheduled meeting with the Digital Markets Advisory Committee. The Commission is not in a position to analyse the patents listed by Apple based on the limited available information within such a short time span. The Commission notes that specification proceedings are subject to stringent legal deadlines and procedural framework. At the time the letter was submitted, the draft decision had already been shared with the members of the Digital Markets Advisory Committee meeting, in line with Article 50 of Regulation (EU) 2022/1925.⁶⁷³ The Commission observes there is no reason for Apple to have submitted the letter this late – the letter does not refer to any new developments or information that Apple would have not had access to during the proceedings. Indeed, Apple should have been able to submit the information in its letter at earlier stage of the proceedings, most notably in its reply to the Preliminary Findings, which makes this hasty submission all the more surprising.

⁶⁷⁰ Apple's reply to the Preliminary Findings, paragraph 103.

⁶⁷¹ See also Section 3.1.1 of this Decision.

⁶⁷² Letter from Apple dated 14 March 2025 (received on 15 March 2025).

⁶⁷³ Article 3(1) of the Rules of procedure for the Digital Markets Advisory Committee sets out that when the Digital Markets Advisory Committee is asked to give an opinion on an implementing act, the meeting must be convened and the draft implementing act must be shared 14 days before the meeting, except for duly justified cases.

- (667) Indeed, the Preliminary Findings set out the scope of these proceedings, in particular the relevant features subject to this Decision. The features covered by these proceedings were communicated to Apple even before the adoption of the Preliminary Findings, on 25 September 2024. [...] In order to ensure the effective application of the Regulation (EU) 2022/1925, the Commission must, within a short time, conclude specification proceedings. Gatekeepers must submit information they deem relevant as soon as possible and within the procedural framework to allow the Commission to conduct a thorough review *within* the administrative proceedings.⁶⁷⁴
- (668) Pursuant to Article 34(2) of Regulation (EU) 2022/1925, gatekeepers may submit their observations on the preliminary findings within a time limit set by the Commission. A timely submission of observations is crucial to provide the Commission with sufficient time for review and assessment, in particular within the context of specification proceedings which are subject to strict procedural rules and timelines.⁶⁷⁵ In this case, the Commission, following Apple's request, set the deadline to reply to the Preliminary Findings to 20 January 2025, following Apple's request for an extension. Apple has had thus one month to reply to the Preliminary Findings and, considering the advance information of the scope of the features covered by these proceedings on 25 September 2024, almost four months to identify any patents or specific IPRs allegedly affected by these proceedings. Apple was also aware of requests submitted through the Apple Interoperability Portal for features covered by these proceedings many months before the opening of proceedings (see Section 4 above).
- (669) Following its reply to the Preliminary Findings, Apple did not inform the Commission that it intends to submit further information on its IPR during these proceedings, let alone at such an extremely late point in time. Apple did not raise would need further time to submit evidence regarding its IPR-related claims, and did not motivate its request for an extension of the deadline to reply to the Preliminary Findings that it would more time for that purpose.
- (670) *Second*, upon a review in the available time, Apple's letter in any event does not sufficiently substantiate its IPR-related concerns to allow the Commission to assess them in detail. [...] ⁶⁷⁶ [...]
- (671) [...] ⁶⁷⁷ For one of these three patents such a relationship does not even seem to exist. [...] ⁶⁷⁸
- (672) As set out in recital (655), Apple is best placed to explain which of its IPRs the measures would interfere with. [...] ⁶⁷⁹ [...] ⁶⁸⁰
- (673) Finally, the Commission notes that the mere existence of a measure interfering with an existing European patent does not automatically exempt the technology from the scope of Article 6(7) of Regulation (EU) 2022/1925. As explained in recital (660),

⁶⁷⁴ Judgment of 17 July 2024, Bytedance v Commission, T-1077/23, EU:T:2024:478, paragraphs 233-237.

⁶⁷⁵ See judgement of 17 July 2024, ByteDance v Commission, T-1077/23, ECLI:EU:T:2024:478, paragraphs 233 and 234, in which the General Court highlighted the need of timely submissions within the deadlines foreseen by Regulation (EU) 2022/1925.

⁶⁷⁶ [...]

⁶⁷⁷ [...]

⁶⁷⁸ [...]

⁶⁷⁹ Letter from Apple dated 14 March 2025 (received on 15 March 2025), pages 4 and 5.

⁶⁸⁰ [...]

the Union legislator has already weighed the public interests against the private interests of economic operators impacted by that legislation, including the degree of legal protection of IPR. The legislator adopted Article 6(7) of Regulation (EU) 2022/1925 without providing for a justification based on IPR. While the Commission is under a duty to comply with the principle of proportionality and fundamental rights guaranteed under the Charter, Article 6(7) of Regulation (EU) 2022/1925 does not mandate an open-ended analysis of the impact of the measures in this Decision on gatekeeper's IPR. Based on Apple's submission, and assuming an interference with an existing European patent, it remains unclear why any proposed measure would disproportionately interfere with such patent.

6.2. Right to compete on privacy and security

- (674) Apple submits that its right to conduct its business and compete on privacy and security grounds is protected by Article 16 of the Charter.⁶⁸¹ Article 16 of the Charter recognises the freedom to conduct business in accordance with Union law and national laws and practices.
- (675) In this respect, Apple makes general assertions about the security of Apple's "integrated system" and refers to risks regarding *"the sharing of Wi-Fi network credentials."* Moreover, Apple refers to its ability *"to ensure that the necessary protections are in place"* and the need to be able *"to ensure that the protections are not simply removed when third-party connected physical devices and related services interoperate with iOS"* to avoid undermining security and privacy. Apple also claims that granting *"third-party access without having the necessary layers of security in place would inevitably create serious and unacceptable risks to the integrity and security of iOS [which is why] Apple needs to be able to choose to build its own solutions, which build in measures to ensure protection of security."* Otherwise, there would be a tension with Regulation (EU) 2016/679; compliance with that Regulation requires *"active steps that ensure that users remain in control of their data."*⁶⁸²
- (676) The Commission notes that Apple did not claim that the proposed measures would breach Article 16 of the Charter but rather would merely interfere with its rights. In any case, Apple's claims are unfounded for the following reasons.
- (677) *First*, Apple's claims on security are general and abstract. They do not relate to the features subject to this Decision and it is unclear how the measures in this Decision, taking into account the possibility of an integrity justification under the second subparagraph of Article 6(7) of Regulation (EU) 2022/1925, would affect Apple's ability to ensure that its own products and those of third parties ensure the protection of security. The only concern that relates to a specific feature concerns the sharing of Wi-Fi network credentials, which is discussed in Section 5.8.6.1 of this Decision. To the extent that Apple raises security concerns in relation to specific features during the administrative proceedings, those are addressed in the section relating to the relevant feature.⁶⁸³
- (678) These claims lack substantiation and plausibility against the background that many features of iOS are already interoperable for third parties, including some with significant security and privacy aspects (e.g. face and fingerprint-based

⁶⁸¹ Apple's reply to the Preliminary Findings, paragraph 27.

⁶⁸² Apple's reply to the Preliminary Findings, paragraphs 24-27, 5.

⁶⁸³ See Sections 5.4.6.3, 5.6.6.3, 5.8.6.1, 5.9.6.3 and 5.11.6.3 of this Decision.

authentication, access to camera and to microphone, access to location, access to photos and health-related data). This has not prevented Apple from making them interoperable. In fact, many of the interoperability requirements specified in this Decision are already implemented, voluntarily and by design, in major operating systems. Apple has not claimed, let alone provided any evidence that such interoperability solutions would have compromised the integrity of such other operating systems or made them insecure.

- (679) *Second*, Apple’s claim regarding a “*tension*” with the requirements of Regulation (EU) 2016/679 is equally general and abstract and therefore unsubstantiated. It is not clear which obligations of Regulation (EU) 2016/679 Apple would not be able to meet as a result of the measures in this Decision. Moreover, as explained in Section 3.3 of this Decision, both Apple and the providers of services or hardware requesting effective interoperability under Article 6(7) of Regulation (EU) 2022/1925 are subject to various legal obligations applicable to their activities concerning, *inter alia*, security or privacy.
- (680) *Third*, Apple does not substantiate why the Commission’s measures would impede Apple’s ability to compete on security and privacy (or on any other aspect). The measures simply require Apple to provide access to the same iOS features that are currently reserved to Apple’s services and hardware. Apple remains free to use those features,⁶⁸⁴ and end users remain free to continue using Apple’s services rather than third-party services.
- (681) *Fourth*, Apple has not substantiated during the administrative proceedings that the proposed measures would interfere disproportionately with Apple’s right under Article 16 of the Charter. In particular, Apple has not explained why any interference by this Decision with its right to operate a business would be of such nature and weight to set aside, in this particular case, the Union legislator’s weighing of the public interests against the private interests of economic operators impacted by that legislation as reflected in the wording of Article 6(7) of Regulation (EU) 2022/1925.

6.3. Other points raised by Apple

- (682) Apple submitted that the inclusion of AWDL in the measures would violate the principle of proportionality.⁶⁸⁵ While in the Preliminary Findings the Commission proposed allowing effective interoperability either by implementing AWDL or Wi-Fi Aware as alternatives, this Decision requires interoperability only with Wi-Fi Aware.⁶⁸⁶ The Commission considers this to be proportionate taking account of Apple’s submissions to this effect.
- (683) As to Apple’s general argument raised during the administrative proceedings that the implementation of the proposed measures would require Apple to significantly invest in time, money, and effort, which would otherwise be used to work on new

⁶⁸⁴ In fact, nothing in this Decision prevents Apple from using the same interoperability solution that it will make available to third-party services and hardware. This means that it is logically impossible for Apple’s services and hardware to be at a disadvantage compared with third-party services and hardware, because Apple has access to no less interoperability solutions than third parties have.

⁶⁸⁵ Apple’s reply to Preliminary Findings, paragraph 8.

⁶⁸⁶ Preliminary Findings, paragraphs 108-111. This Decision does not take a position whether, and under what circumstances, Apple must allow interoperability under Article 6(7) of Regulation (EU) 2022/1925 with AWDL, particularly if the measures specified in this Decision prove not to be effective.

innovations to the detriment of Apple,⁶⁸⁷ the Commission notes that this argument in essence challenges the legality and the proportionality of Regulation (EU) 2022/1925 itself, which is the subject matter of Apple’s pending application for annulment submitted pursuant to Article 263 TFEU against Commission Decision C(2023) 2746 final of 5 September 2023 designating Apple as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925.⁶⁸⁸ In the context of this case, Apple did not explain why these investments would be of such nature and weight to set aside, in this particular case, the Union legislator’s weighing of the public interests against the private interests of economic operators impacted by that legislation as reflected in the wording of Article 6(7) of Regulation (EU) 2022/1925, particularly given that allowing for effective interoperability typically requires a certain amount of time, money, and effort.

- (684) Moreover, Apple considered the deadlines for the implementation of the proposed measures as too short and unfeasible.⁶⁸⁹ The Commission notes, *first*, that Apple has had at least since the designation of its operating system iOS as a regulated core platform service under Regulation (EU) 2022/1925 to prepare for the implementation of interoperability solutions and equip itself with the necessary resources to develop such solutions.⁶⁹⁰ *Second*, Apple has had a significant amount of time to work on specific interoperability solutions for features within the scope of this Decision. Most of the interoperability requests for the respective features have reached Apple several months ago, sometime more than a year ago.⁶⁹¹ *Third*, [...].⁶⁹² Nevertheless, the Commission recognises that the implementation of effective interoperability requires time and resources, and that some potential technical difficulties may arise, which will have to be overcome. As a result, and following additional discussions with Apple, the Commission further extended most timelines in this Decision, in line with Apple’s submissions.⁶⁹³
- (685) Finally, Apple’s innovation arguments are addressed in Section 3.2 of this Decision and Apple’s arguments regarding future updates are addressed in Section 3.1.3 of this Decision. In neither case has Apple demonstrated that the measures in this

⁶⁸⁷ Apple’s reply to Preliminary Findings, paragraph 39.

⁶⁸⁸ Case T-1080/23.

⁶⁸⁹ Apple’s reply to Preliminary Findings, paragraph 39.

⁶⁹⁰ There is no indication and Apple does not claim that it was impossible for Apple to equip itself with the necessary resources. See, by analogy, judgment of 25 February 2025, Alphabet v AGCM, C-233/23, ECLI:EU:C:2025:110, paragraph 75.

⁶⁹¹ See, for example, recital (173) of this Decision.

⁶⁹² Email from Apple to the Commission of 3 February 2025 [...]; see also [...] in an email from Apple to the Commission on 17 February 2025 [on draft final measures].

⁶⁹³ The Decision relaxes the implementation timelines compared to the preliminary findings for the features of proximity-triggered pairing (Section 5.5.8 of this Decision), close-range wireless file transfer (Section 5.7.8 of this Decision), automatic Wi-Fi connection (Section 5.8.8 of this Decision), media casting (Section 5.9.8 of this Decision), automatic audio switching (Section 5.10.8 of this Decision), NFC controller in Reader/Writer mode (Section 5.11.8 of this Decision), and partially as well for iOS notifications (Section 5.3.8 of this Decision), high-bandwidth peer-to-peer Wi-Fi connection (Section 5.4.8 of this Decision) and background execution (Section 5.6.8 of this Decision), while also deviating in some cases [...]: for the high-bandwidth peer-to-peer Wi-Fi connection feature (reasons set out in Section 5.4.6.6 of this Decision), the close-range wireless file transfer features (reasons set out in Section 5.7.6 of this Decision), the access to the NFC controller in Reader/Writer mode feature (reasons set out in Section 5.11.6.4 of this Decision) and the automatic audio switching feature (reasons set out in Section 5.10.6 of this Decision). The reasons for the timing for the registration process for the proximity-triggered pairing feature are set out in Section 5.5.6 of this Decision.

Decision would significantly reduce – or even less remove – Apple’s incentives to innovate.⁶⁹⁴ Apple has also not explained why Apple’s concerns in this regard are of such nature and weight to set aside, in this particular case, the Union legislator’s weighing of the public interests against the private interests of economic operators impacted by that legislation as reflected in the wording of Article 6(7) of Regulation (EU) 2022/1925.

- (686) On this basis, the Commission considers that it has discharged its duty to comply with the principle of proportionality in the measures in the Annex to this Decision.

7. CONCLUSION

- (687) For the reasons set out above, the Commission hereby specifies measures pursuant to Article 8(2) of Regulation (EU) 2022/1925 that Apple has to implement within the deadlines specified in the Annex to this Decision to effectively comply with the obligations under Article 6(7) of Regulation (EU) 2022/1925 in relation to certain iOS features for connected physical devices.

HAS ADOPTED THIS DECISION:

Article 1

Apple shall implement the measures as specified in the Annex to this Decision within the deadlines specified therein pursuant to Article 8(2) of Regulation (EU) 2022/1925.

Article 2

This Decision is addressed to Apple Inc., One Apple Park Way, Cupertino, CA 95014, United States of America, and Apple Distribution International Limited, Hollyhill Industrial Estate, Hollyhill, Cork, Ireland.

Done at Brussels, 19.3.2025

For the Commission

Signed

Teresa RIBERA

Executive Vice-President

⁶⁹⁴ Judgment of 17 September 2007, Microsoft v Commission, T-201/04, EU:T:2007:289, paragraph 701.

**DMA.100203 – Apple – Operating Systems – iOS – Article 6(7) – SP – Features for
Connected Physical Devices**

Decision of 19 March 2025 – Final Measures

Non-Confidential Version

[This version has been adapted for publication. Only the adopted decision is legally binding.]

Table of Contents

1. IOS NOTIFICATIONS.....	1
2. HIGH-BANDWIDTH PEER-TO-PEER WI-FI CONNECTION	4
3. PROXIMITY-TRIGGERED PAIRING	7
4. BACKGROUND EXECUTION.....	9
5. CLOSE-RANGE WIRELESS FILE TRANSFER	11
6. AUTOMATIC WI-FI CONNECTION	15
7. MEDIA CASTING	17
8. AUTOMATIC AUDIO SWITCHING.....	18
9. NFC CONTROLLER IN READER/WRITER MODE	20

1. iOS NOTIFICATIONS

- (1) Apple shall provide effective interoperability with the iOS notifications feature.
- (2) The iOS notifications feature is described in Section 5.3.1 of the Decision. The feature enables Apple’s hardware and services, including Apple’s connected physical devices, to receive, access, use, respond to, and transmit iOS notifications as well as to select and manage which notifications are displayed. An iOS notification is a message, icon or another symbol that iOS displays or can display on an iOS device, by showing an alert, playing a sound, or badging the icon of an app sending the iOS notification. End users have access to settings regarding iOS notifications, which include the possibility for end users to configure if and how, and which iOS notifications are forwarded to the connected physical device. On the Apple connected physical device, end users can reply to and interact with iOS notifications (e.g. to accept or decline a calendar invitation), with the reaction being reflected on the iOS device (e.g. in the calendar app).
- (3) Apple shall implement an interoperability solution that provides third parties with access to the same iOS notifications feature described in the preceding paragraph

and Section 5.3.1 of the Decision as available to Apple, in a way that is equally effective as the solution available to Apple.

- (4) Apple shall provide effective interoperability with all functionalities of the iOS notifications feature which are available to Apple's own connected physical devices, including, but not limited to, AirPods, Apple Watch, Apple Vision Pro, as well as any future Apple connected physical devices. These functionalities are:
 - (a) receiving iOS notifications on the connected physical device and taking actions in response to iOS notifications, including custom actions defined by the third-party developer, on the connected physical device to ensure that the response or interaction is registered and reflected by the iOS device;
 - (b) selecting which iOS notifications are shown on each connected physical device within the companion app of the respective connected physical device or iOS settings, at the developer's option; and
 - (c) displaying logos associated with the app posting the iOS notification and images, attachments and other metadata associated with the iOS notification on the connected physical device.
- (5) Apple shall grant third parties access to additional functionalities if necessary to enable effective interoperability with the iOS notifications feature referred to in paragraph (3) of this Annex.
- (6) To provide third parties with an interoperability solution for the iOS notifications feature referred to in paragraph (3) of this Annex that is equally effective as that available to any of Apple's own connected physical devices, Apple shall implement the following measures.
 - (a) Apple shall provide third-party iOS apps, in particular companion apps of connected physical devices, with the full and complete payload¹ and metadata² of all iOS notifications. The third party and the end user must then be able to decide whether and how an iOS notification is relayed to the third-party connected physical device. To ensure interoperability under equal conditions with Apple's connected physical devices, Apple should ensure that the third party is able to pre-process in its iOS app the iOS notifications, for example to adjust the size of an image or summarise a text, before the iOS notification is relayed to the third-party connected physical device. Apple is allowed to require that third-party developers encrypt the iOS notification before relaying it to the connected physical device.
 - (b) Apple shall ensure that third parties are free to decide which transport technology they want to use to relay the iOS notification to the connected

¹ The payload contains the custom iOS notification data including the delivery content and information about how iOS should notify the user.

² Enabling, for example, the display of logos associated with the app posting the iOS notification as well as images and attachments associated with the iOS notification on the connected physical device.

physical device (e.g. Bluetooth only or other technologies such as infrastructure Wi-Fi, peer-to-peer Wi-Fi or cellular connections).

- (c) Apple shall allow third parties to implement in their iOS app, or Apple shall make available in iOS settings, at the developer's option, functionality which enables end users to decide which iOS notifications from which apps are relayed to the third-party connected physical device. Apple shall also allow third parties to implement in their iOS app a functionality which enables end users to decide whether iOS notifications from a given app should be shown or not shown at certain times or under certain conditions (e.g. during certain activities or times of the day).
- (7) Apple shall ensure that any interoperability solution for iOS notifications does not require any changes or further implementation to apps posting iOS notifications.³ To the extent the developer of an app sending iOS notifications has enabled certain functionalities or settings for the relay and showing of its iOS notifications on Apple's connected physical devices, in particular the Apple Watch, these must automatically and to the same extent be available to third parties.⁴
- (8) Apple shall also provide effective interoperability with any future updates, including new functionalities, of the iOS notifications feature insofar as they are available to Apple's own connected physical devices. To this end, the general measures in paragraph (101) of this Annex apply, including in particular the measures concerning future updates and new functionalities set out in paragraph (101)(j) of this Annex. To the current knowledge of the Commission, future or recently introduced functionalities of the iOS notifications feature include:
 - (a) prioritising certain notifications on top of the screen of the connected physical device (so called "Priority Notifications"); and
 - (b) showing a summary of non-emergency notification at scheduled times (so called "Summary Notifications").
- (9) Apple shall implement the measures above in compliance with the measures for all features in Section 10 of this Annex.
- (10) Apple shall implement the measures for the iOS notifications feature (except for (i) the ability to select which iOS notifications are shown on each connected physical device within the companion app, and (ii) the functionalities described in paragraph (8) of this Annex) in a beta version of iOS available to developers by the end of 2025

³ Neither from developers of apps posting iOS notifications or of their end users. In particular, Apple may not require developers to change or add the programming of the payload of their iOS notifications.

⁴ For example, if a messaging app developer has defined certain parameters for the showing of its iOS notifications – such as the headline, icon, or play sound – the same notification with the same parameters must be available out-of-the-box to third-party smartwatches, without the need for the messaging app developer to make special changes to their app in order to support third-party connected physical devices.

at the latest. Apple shall thereafter implement all measures for the iOS notifications feature by 1 June 2026 at the latest.

2. HIGH-BANDWIDTH PEER-TO-PEER WI-FI CONNECTION

- (11) Apple shall provide effective interoperability with the high-bandwidth peer-to-peer Wi-Fi connection feature (hereinafter referred to as “P2P Wi-Fi connection feature”).
- (12) The P2P Wi-Fi connection feature is described in Section 5.4.1 of the Decision. The feature enables iOS devices to establish and use a P2P Wi-Fi connection with another Apple device that supports the same P2P Wi-Fi communication protocol. The P2P Wi-Fi connection connects devices to transfer data without an intermediary, meaning that the P2P Wi-Fi connection works independently of either of the involved devices being connected to any local infrastructure Wi-Fi or cellular network. Furthermore, the P2P Wi-Fi connection can work concurrently with an infrastructure Wi-Fi connection. This means that an iOS device can be connected to a connected physical device via a P2P Wi-Fi connection, while maintaining a connection with infrastructure Wi-Fi. Apple implemented and uses the P2P Wi-Fi communication protocols AWDL and Wi-Fi Aware on iOS devices.
- (13) Apple shall implement an interoperability solution that provides third parties with access to the same high-bandwidth P2P Wi-Fi feature described in the preceding paragraph and Section 5.4.1 of the Decision as available to Apple, in a way that is equally effective as the solution available to Apple. For the avoidance of doubt, this includes using the P2P Wi-Fi connection feature between an iOS device and a nearby Apple or third-party connected physical device.
- (14) Apple shall provide interoperability with all functionalities of the high-bandwidth P2P Wi-Fi connection feature which are available to Apple’s own connected physical devices, including, but not limited to, Apple Vision Pro, Apple Watch, as well as any future Apple connected physical devices. These functionalities are:
 - (a) initiating a P2P Wi-Fi connection by discovering⁵ nearby connected physical devices and securely pairing⁶ with a nearby connected physical device via P2P Wi-Fi;
 - (b) establishing a P2P Wi-Fi connection with high bandwidth, high speed, and latency, that does not have a central coordinator, and that can be maintained for the same amount of time as is available to Apple;

⁵ “Device discovery” refers to the ability of a device, whether it is an iPhone or a connected physical device, to discover or be discovered by nearby devices, e.g. by sending or listening to Bluetooth signals. Device discovery may be automatic or may follow explicit user action. Device discovery is essential in order to subsequently pair two devices and establish a connection between those devices.

⁶ “Pairing” refers to the process of connecting two nearby devices to establish a communication channel between the two devices. Nearby devices can typically be paired if they have either just discovered each other or have a trusted relationship.

- (c) establishing a P2P Wi-Fi connection that can run independently and concurrently to infrastructure Wi-Fi (e.g. via internet router or, if Apple makes such a hotspot available to any of its own connected physical devices, hotspot provided by the iOS device or connected physical device) via channel switching, as well as synchronization to improve the performance of channel switching;
 - (d) establishing a P2P Wi-Fi connection that serves as a hotspot providing internet access to a connected physical device using a concurrent connection (e.g. cellular), if Apple makes such a functionality available to any of its own connected physical devices;
 - (e) establishing multiple concurrent P2P Wi-Fi connections without discontinuing existing P2P Wi-Fi connections between an iOS device and connected physical devices;
 - (f) establishing a P2P Wi-Fi connection upon request of the relevant third-party iOS app, without further user intervention via the companion app or otherwise, or without more user intervention than is required between Apple devices for a P2P Wi-Fi connection;
 - (g) allowing the P2P Wi-Fi connection between trusted devices⁷ to run in the background after initiation, without the need for the app(s) initiating the P2P Wi-Fi connection to be in the foreground;
 - (h) once established, allowing iOS apps to use the P2P Wi-Fi connection, to access the same connection metadata, and to allow third parties to configure the same parameters of the Wi-Fi Aware connection as Apple uses itself in its P2P Wi-Fi connection solution;
 - (i) disabling the P2P Wi-Fi connection automatically once the use case is completed in order to save battery power and Wi-Fi bandwidth.
- (15) Apple shall grant third parties access to additional functionalities if necessary to enable effective interoperability with the P2P Wi-Fi connection feature referred to in paragraph (13) of this Annex.
- (16) Apple shall make Wi-Fi Aware available to third parties.
- (17) Implementing a solution based on the use of Wi-Fi Aware means that Apple shall allow third-party connected physical devices access to the same functionalities of the P2P Wi-Fi connection feature as available to Apple's own connected physical devices. This means in practice that Apple shall:
- (a) implement Wi-Fi Aware in its iOS devices and iOS in accordance with the Wi-Fi Aware specification unless Apple demonstrates that it is not necessary to ensure that third parties have access to the same functionalities and in an

⁷ A "trusted device" is another device with which a device has a trusted relationship. Devices may establish a trusted relationship before or during the pairing process.

equally effective way as Apple's own connected physical devices under its own implementation of P2P Wi-Fi;

- (b) allow third parties to establish a Wi-Fi Aware connection between an iOS device and any third-party connected physical device that supports Wi-Fi Aware;
 - (c) allow third parties to establish a Wi-Fi Aware connection on-demand, without further user intervention via the companion app or otherwise, or without more user intervention than is required between Apple devices to establish a P2P Wi-Fi connection;
 - (d) allow third parties to establish a Wi-Fi Aware P2P connection with an iOS device, while the iOS device can maintain an infrastructure Wi-Fi connection in parallel. Furthermore, Apple shall implement a non-discriminatory channel switching policy that is most suitable for its own and third-party use cases;
 - (e) allow third parties access to the same connection metadata and to configure the same parameters of the Wi-Fi Aware connection as Apple uses itself in its P2P Wi-Fi connection solution;
 - (f) to the extent technically possible, ensure that the Wi-Fi chip of iOS devices, including legacy devices, allocate the memory available to support two concurrent P2P Wi-Fi connections in a non-discriminatory way, until Apple deprecates AWDL;
 - (g) continue to constructively engage with Wi-Fi Alliance participants to further improve the Wi-Fi Aware standard regarding any functionality available to Apple's own connected physical devices under its own implementation of P2P Wi-Fi; in the absence of legitimate and substantiated intellectual property right concerns, Apple shall not prevent, explicitly or de facto, functionalities available under its own implementation of P2P Wi-Fi from becoming part of the Wi-Fi Aware standard;
 - (h) update the iOS Wi-Fi Aware implementation to support the newest Wi-Fi Aware standard after its adoption by the Wi-Fi Alliance within a reasonable timeframe regarding any functionality available to Apple's own connected physical devices under its own implementation of P2P Wi-Fi, unless Apple demonstrates that effective interoperability with the same functionality already exists; for the avoidance of doubt, this includes supporting the wireless communication standards that are available to Apple's own connected physical devices.
- (18) To the extent technically possible, Apple shall provide third parties with a Wi-Fi Aware implementation in a way that is equally effective as its own implementation of P2P Wi-Fi. Until AWDL is deprecated, Apple must ensure, to the extent technically possible, that the solution made available to third parties is equally effective to the solution made available to Apple's connected physical devices, including in terms of set-up speed, bandwidth, transfer speed, performance, latency and uptime.

- (19) Apple shall also provide effective interoperability with any future updates, including new functionalities, of the P2P Wi-Fi connection feature, including with future functionalities of AWDL, insofar they are available to Apple's own connected physical devices. To this end, the general measures in paragraph (101) of this Annex apply, including in particular the measures concerning future updates and new functionalities set out in paragraph (101)(j) of this Annex. This applies regardless of whether the future functionalities are part of the Wi-Fi Aware standard, unless Apple demonstrates that it is not possible to incorporate them into the P2P Wi-Fi implementation based on Wi-Fi Aware. In addition, subject to legitimate and substantiated intellectual property right concerns, Apple shall not prevent, explicitly or de facto, future updates, including new functionalities, of AWDL from becoming part of the Wi-Fi Aware standard. Future functionalities of the P2P Wi-Fi connection feature include:
- (a) [confidential]
 - (b) [confidential]
- (20) Apple shall implement the measures above in compliance with the measures for all features in Section 10 of this Annex.
- (21) Apple shall implement the measures for Wi-Fi Aware 4.0 in the next major iOS release, i.e. iOS 19, at the latest, and for Wi-Fi Aware 5.0 in the next iOS release at the latest nine months following the introduction of the Wi-Fi Aware 5.0 specification.

3. PROXIMITY-TRIGGERED PAIRING

- (22) Apple shall provide effective interoperability with the proximity-triggered pairing feature.
- (23) The proximity-triggered pairing feature is described in Section 5.5.1 of the Decision. The proximity-triggered pairing feature enables the pairing and setup of Apple connected physical devices with an iOS device via a proximity-triggered procedure through a streamlined user-friendly process. Proximity-triggered pairing works out of the box: there is no need for the user to install any app beforehand and the feature automatically works for any connected physical device for which Apple has implemented support, including the Apple Watch and AirPods.
- (24) Apple shall implement an interoperability solution that provides third parties with access to the same proximity-triggered pairing feature described in the preceding paragraph and Section 5.5.1 of the Decision as available to Apple, in a way that is equally effective as the solution available to Apple's own connected devices.
- (25) Apple shall provide interoperability with all functionalities of the proximity-triggered pairing feature which are available to Apple's own connected physical devices, including, but not limited to, AirPods, Apple Vision Pro, Apple Watch, as well as any future Apple connected physical devices. These functionalities are:
- (a) the ability of a third-party connected physical device to establish a Bluetooth connection with an iOS device for pairing purposes;

- (b) the ability for the pairing process between the third-party connected physical devices and the iOS device to be triggered by the proximity of the connected physical device to the iOS device;
 - (c) the ability for the third-party connected physical device to be automatically discovered by the iOS device via the BLE protocol for the initiation of the pairing process without the need for the end user to first download a third-party companion app;
 - (d) the ability to carry out the pairing and setup of the third-party connected physical device with the iOS device as a continuous and guided process starting with the proximity-triggered detection and, at the third party's option, continuing within the third-party companion app;
 - (e) The ability to make use of the same end user journey and ease of use for end users, as technically possible given the possible need to install a companion app, which includes:
 - (i) showing the same user prompts (in terms of, *inter alia*, number, content, format and design) as shown for Apple's most comparable connected physical device;
 - (ii) showing the same information screens (in terms of, *inter alia*, number, content, format and design) as shown for Apple's most comparable connected physical device, in as much this is feasible considering the device capability;
 - (iii) limiting the necessary time and user engagement to the same level as required for pairing Apple's most comparable connected physical device, including the number of prompts and information screens; in particular, where the end user is prompted to initiate the pairing process with a third-party connected physical device, the third-party companion app of the third-party connected physical device must be capable of being opened or downloaded, at the determination of the third-party developer, seamlessly without an additional user prompt unless Apple shows an equivalent prompt for its own connected physical devices;
 - (f) the settings regarding device pairing, including the location of the settings (e.g. in iOS settings or in an app) and the scope of settings.
- (26) Apple shall grant third parties access to additional functionalities if necessary to enable effective interoperability with the proximity-triggered pairing feature referred to in paragraph (24) of this Annex.
- (27) To enable out-of-the-box proximity-triggered device discovery, Apple may integrate a mapping between third-party connected physical devices and the expected contents of their BLE advertisements, the relevant companion app(s), as well as other necessary metadata (including, but not limited to, transmission power or security keys) into iOS. To obtain the necessary metadata for this mapping, Apple may set up a program for third-party connected physical device manufacturers to register their connected physical devices for the purpose of making use of the proximity-

triggered pairing feature. Apple shall ensure that such devices are registered and can use the proximity-triggered pairing feature within 15 days following the submission of the registration request. In the event of circumstances beyond Apple's control, Apple shall make best efforts to register the devices as soon as possible and not later than within four weeks following the submission of the registration request.

- (28) Apple shall also provide effective interoperability with any future updates, including new functionalities, of the proximity-triggered pairing feature insofar as they are available to Apple's own connected physical devices. To this end, the general measures in paragraph (101) of this Annex apply, including in particular the measures concerning future updates and new functionalities set out in paragraph (101)(j) of this Annex.
- (29) Apple shall implement the measures above in compliance with the measures for all features in Section 10 of this Annex.
- (30) Apple shall implement the measures for the proximity-triggered pairing feature in a beta version of iOS available to developers by the end of 2025 at the latest. Apple shall then implement the measures for the proximity triggered feature for end users by 1 June 2026 at the latest.

4. BACKGROUND EXECUTION

- (31) Apple shall provide effective interoperability with the background execution feature in relation to connected physical devices and related apps.
- (32) The background execution feature is described in Section 5.6.1 of the Decision. The feature consists in the ability to timely execute actions on and communicate with an iOS device with respect to Apple connected physical devices, without the need for the iOS device to have the screen on or for a specific app to be in the foreground. The background execution feature allows Apple's services and hardware to access relevant iOS interfaces and resources regardless of whether an active end user interaction took place (e.g. after an iPhone is switched on, or when the screens of the iPhone and/or connected physical device are locked). In particular, it allows Apple to ensure that the iOS device can reliably continuously scan for Bluetooth Low Energy ("BLE") advertisement from connected physical devices; establish and maintain a connection with connected physical devices; have network access for purposes related to connected physical devices, e.g. to send and receive data via the internet; and process data for interaction with connected physical devices.
- (33) Apple shall allow third parties effective interoperability with the same background execution feature described in the preceding paragraph and Section 5.6.1 of the Decision as available to Apple, in a way that is equally effective as the solution available to Apple.
- (34) Apple shall provide interoperability with all functionalities of the background execution feature which are available to Apple's own connected physical devices, including, but not limited to, AirPods, Apple Vision Pro, Apple Watch, as well as any future Apple connected physical devices. Apple should provide interoperability with the following functionalities.

- (a) Apple shall grant iOS companion apps,⁸ iOS sister apps,⁹ and relevant iOS processes the same background execution capabilities on iOS devices to execute actions with respect to third-party connected physical devices that Apple grants, including via iOS processes and iOS daemons, to execute actions with respect to Apple's connected physical devices. This includes any restrictions, time windows, and resource limitations (e.g. on CPU and/or GPU execution), which Apple shall apply according to transparent, objective, precise, and non-discriminatory rules that also apply to Apple's services and hardware, including for use cases that Apple does not offer.
- (b) Any limitation or choice on the background execution capabilities of third-party iOS companion apps, iOS sister apps, or relevant iOS processes with respect to third-party connected physical devices as a result of a user action shall only be permissible if the user can take the same action with the same limiting effect regarding Apple's most comparable connected physical devices. This includes the action of a user terminating a companion or sister app in the app switching menu ("force-quitting") and the action of disabling Wi-Fi or Bluetooth through iOS Control Centre, as well as the resulting impact on background execution with the connected physical device.
- (c) Apple shall grant third-party iOS companion apps and iOS sister apps equal use of background execution functionalities – regardless of whether an active end user interaction took place¹⁰ – under transparent, objective, precise, and non-discriminatory rules that also apply to Apple's services and hardware, including for use cases that Apple does not offer. These functionalities include:
 - (i) having the iOS device constantly listen for signals from the third-party connected physical device based on BLE and any other communication protocol that Apple uses to scan for advertisements from the connected physical device;
 - (ii) allowing the iOS companion app or iOS sister app to timely establish, maintain and use a connection between the iOS device and the third-

⁸ An 'iOS companion app' is an iOS app that facilitates the use of connected physical devices, such as the pairing between an iPhone and the connected physical device, setup of the connected physical device, controlling functionalities of the connected physical device, or offering services relating to the use of the connected physical device.

⁹ A 'sister app' is an app that is designed to communicate with a corresponding app on another device. An iOS sister app is then an iOS app that is designed to communicate with a corresponding app on a connected physical device. For instance, the user may install the same fitness app from an app developer both on the iOS device and a smartwatch, with the two apps being designed to transmit data to each other, for instance to keep fitness statistics synchronised.

¹⁰ For example, after an iPhone is switched on or when the screens of the iPhone and/or connected physical device are locked.

party connected physical device to transmit data between the app and the third-party connected physical device; and

- (iii) allowing the iOS companion app and iOS sister app network access on the iOS device, including to send and receive data from internet servers, for purposes related to the connected physical device.
- (35) Apple may continue to require user permission for Bluetooth access APIs that currently require such user permission, in compliance with the requirements of Article 6(7) of Regulation (EU) 2022/1925.
- (36) Apple shall grant third parties access to additional functionalities if necessary to enable effective interoperability with the background execution feature referred to in paragraph (33) of this Annex.
- (37) Apple shall also provide effective interoperability with any future updates, including new functionalities, of the background execution feature insofar as they are available to Apple's own connected physical devices. To this end, the general measures in paragraph (101) of this Annex apply, including in particular the measures concerning future updates and new functionalities set out in paragraph (101)(j) of this Annex.
- (38) Apple shall implement the measures above in compliance with the measures for all features in Section 10 of this Annex.
- (39) Apple shall implement the measures concerning background execution for third-party companion apps in relation to force-quitting and Bluetooth/Wi-Fi disabling actions in the next major iOS release, i.e. iOS 19, and in any case by the end of 2025 at the latest, and all of the measures for the background execution feature in the release of iOS 20, and in any case by the end of 2026 at the latest.

5. CLOSE-RANGE WIRELESS FILE TRANSFER

- (40) Apple shall provide effective interoperability with the features for close-range wireless file transfer solutions.
- (41) The features for close-range wireless file transfer solutions are described in Section 5.7.1 of the Decision. The features allow Apple to provide feature-rich close-range wireless file transfer solutions, such as AirDrop, to Apple's services and hardware. Close-range wireless file transfers solutions, such as AirDrop, allow iOS devices to transfer files (or more generically "items"), such as photos, URLs, or documents, between nearby Apple connected physical devices. Furthermore, close-range wireless file transfer solutions encompass the ability to pair nearby devices and have access to several communication protocols to transfer files (e.g. P2P Wi-Fi, infrastructure Wi-Fi). Pairing can both establish trust between devices or be facilitated through previously established trust.
- (42) Apple shall implement an interoperability solution that provides third parties with access to the same features for close-range wireless file transfer described in the preceding paragraph and Section 5.7.1 of the Decision as available to Apple, in a way that is equally effective as the solution available to Apple. For the avoidance of

doubt, this includes using file sharing between an iOS device and a nearby Apple or third-party connected physical device.

- (43) Apple shall allow third parties effective interoperability with the same features for close-range wireless file transfer solutions controlled by iOS and their functionalities as available to Apple's own connected physical devices (including via AirDrop), including, but not limited to, Apple Watch, Apple Vision Pro, as well as any future Apple connected physical devices. Apple shall implement an interoperability solution that is equally effective as the solution available to Apple. To that end, Apple shall make the following features available to third-party close-range wireless file transfer solutions.
- (a) Accessibility. The ability of close-range wireless file transfer solutions to be displayed and easily accessible in Apple and third-party services and hardware on an iOS device.
 - (b) Advertisement and device discovery. The ability of close-range wireless file transfer solutions to use a communication protocol to discover and be discovered by nearby Apple and non-Apple devices.
 - (c) Trusted devices. The ability of close-range wireless file transfer solutions to establish trust via the operating system with another device and subsequently filter incoming file transfer requests based on whether the shared file is being sent from a device that is trusted. A trusted device may be an Apple or non-Apple connected physical device.
 - (d) Protocols. The ability of close-range wireless file transfer solutions to establish and use the most appropriate available connection between an iOS device and an Apple or non-Apple connected physical device via a communication protocol or via a file sharing protocol that is based on a communication protocol.
 - (e) Background execution. The ability of close-range wireless file transfer solutions to initiate a file transfer via interfaces supported in iOS that do not require the launching of a separate app, or to execute and continue file sharing in the background if previously initiated by the end user. Any user interface displaying the progress of the file transfer shown to the end user using a third-party solution shall be under equal conditions as when using an Apple solution such as AirDrop, both on the sending and the receiving device.
 - (f) File context. The ability of close-range wireless file transfer solutions to launch the app from which a file was shared using a close-range wireless file transfer solution and store the file in that app, or another app appropriate for the file type in case the corresponding app is not installed on the receiving device.
- (44) To provide third parties with an interoperability solution for iOS features of close-range wireless file transfer solutions that is equally effective as that available to any of Apple's own connected physical devices, Apple shall implement the following measures.
- (45) Accessibility

- (a) Apple shall allow close-range wireless file transfer solutions to be displayed via the same user interface (e.g. iOS Share Sheet) and under the same conditions as Apple's wireless file transfer services, such as AirDrop, are displayed.
 - (b) Apple shall allow third-party close-range file transfer solutions to launch a close-range wireless file transfer by tapping on the respective service in the relevant iOS user interface as available to Apple (e.g. iOS Share Sheet), which ultimately allows the end user to use the solution without the need to open the third-party solution into the foreground.
 - (c) Apple shall allow third-party close-range file transfer solutions to trigger the system user interface responsible for the file transfer on the sending or receiving iOS device, provided that the receiving device has the solution installed. This may include a user experience to trigger device pairing or a notification to launch and connect a close-range wireless file transfer solution. The user experience for the end user using a third-party solution should be under equal conditions as when using an Apple solution such as AirDrop, both on the sending and the receiving device.
 - (d) In the event that the close-range wireless file transfer solution is not installed on the receiving device, Apple shall allow the sending device to discover the paired receiving device, and shall allow the user of the receiving device to be informed of an incoming file (e.g. via a notification, app clip, system user interface) and to be guided to the appropriate app store in order to facilitate the installation of the close-range wireless file transfer solution.
 - (e) Apple shall allow the end user to set the same options and preferences in settings for third-party close-range file transfer solutions, including selecting between "Everyone" and "Contacts only" and adjusting the time limitations of the Everyone Mode, as are available to Apple. Apple shall treat these settings in the same way as it treats settings for its own close-range wireless file transfer solutions, such as AirDrop.
- (46) Advertisement and device discovery
- (a) Apple shall allow close-range wireless file transfer solutions to discover nearby Apple and non-Apple connected physical devices using protocols that include, but are not limited to, BLE, a P2P Wi-Fi connection, and NFC.
 - (b) Apple shall allow third-party connected physical devices to discover nearby iOS devices for close-range wireless file transfers using protocols that include, but are not limited to, BLE, a P2P Wi-Fi connection, and NFC.
 - (c) Apple shall allow close-range wireless file transfer solutions access to the iOS functionality that scans for advertisements for close-range wireless file transfers from nearby connected physical devices under equal conditions as is available to Apple's own close-range wireless file transfer solutions, such as AirDrop (e.g. that both devices have their screen on).
- (47) Trusted devices

- (a) Apple shall allow close-range wireless file transfer solutions to trust a device via the operating system, such that future file transfers do not require re-establishing this trust. Subject to revokable end user consent, the device should remain trusted. Furthermore, the process for third-party solutions to trust another device shall be subject to equal conditions as available to Apple's solutions, such as AirDrop, including the user experience for trusting devices that belong to the same end user or trusting devices from the end user's contacts.
 - (b) Apple shall allow close-range wireless file transfer solutions to limit device discovery of nearby connected physical devices to devices that the end user has previously trusted, regardless of whether the trusted device is an Apple or third-party device, based on the user's choice for the device discovery mode.
- (48) Protocols
- (a) Apple shall allow close-range wireless file transfer solutions to use any communication protocol available to Apple's services or hardware, which includes but is not limited to, BLE, infrastructure Wi-Fi, cellular network and P2P Wi-Fi connection, to transfer files between the iOS device and nearby Apple or third-party connected physical devices (and vice-versa).
 - (b) Apple shall allow close-range wireless file transfer solutions to integrate their own file transfer protocols based on communication protocols.
 - (c) Apple shall allow close-range wireless file transfer solutions to change the communication protocol, for instance in the case where a faster alternative communication channel is available, and providing third-party solutions with the relevant information in order to make such a decision.
 - (d) Apple shall allow close-range wireless file transfer solutions to continue file sharing if the devices involved in the file transfer move out of wireless range using any other available connection (e.g. infrastructure Wi-Fi, cellular network), and provide the relevant connection metadata to indicate that the devices moved out of wireless range.
- (49) Background execution
- (a) Apple shall allow third-party close-range wireless file transfer solutions with the same background execution abilities as are available to Apple's solutions, such as AirDrop. This includes, but is not limited to, the ability to launch the file sharing protocol without needing to open the close-range wireless file transfer solution (e.g. via the iOS Share Sheet) to send or receive files.
 - (b) Apple shall allow close-range wireless file transfer solutions to continue receiving and sending files that are being transferred in the background after the transfer started, meaning that the app in which the file transfer was initiated does not need to remain in the foreground. Apple may require that the progress of the file transfer is presented to the user while it is ongoing and the iPhone screen is on, as long as Apple's solutions, such as AirDrop, are subject to the

same requirement and the close-range wireless file transfer solution can do so through an equivalent interface to Apple's solutions.

- (50) File context. Apple shall allow close-range wireless file transfer solutions to open and store the receiving file under equal conditions as Apple's solutions, such as AirDrop, are capable of opening and storing a receiving file. This could, for instance, include sharing relevant metadata alongside the file that is also available to Apple's connected physical devices, or prompting an end user to open the received file in a specific app.
- (51) Apple shall grant third parties access to additional functionalities if necessary to enable effective interoperability with the features for close-range wireless file transfer solutions referred to in paragraph (42) of this Annex.
- (52) Apple shall also provide effective interoperability with any future updates, including new functionalities, of the iOS features used for close-range wireless file transfer solutions insofar as they are available to Apple's own connected physical devices. To this end, the general measures in paragraph (101) of this Annex apply, including in particular the measures concerning future updates and new functionalities set out in paragraph (101)(j) of this Annex.
- (53) Apple shall implement the measures above in compliance with the measures for all features in Section 10 of this Annex.
- (54) Apple shall implement the measures required to enable the scenario of close-range wireless file transfers while the receiving device has the relevant close-range wireless file transfer solution open by 1 June 2026. Apple shall implement all measures for the features for close-range wireless file transfer solutions in the release of iOS 20, and in any case by the end of 2026.

6. AUTOMATIC WI-FI CONNECTION

- (55) Apple shall provide effective interoperability with the automatic Wi-Fi connection feature.
- (56) The automatic Wi-Fi connection feature is described in Section 5.8.1 of the Decision. The feature allows Apple's connected physical devices to access and use information (including metadata) about certain local infrastructure Wi-Fi networks saved on the iOS device, to allow them to join these networks easily and without friction. An iOS device transmits this information to Apple connected physical devices, such as the Apple Watch, which use this information to establish a local infrastructure Wi-Fi connection, without the user having to select a Wi-Fi network on that device, and without the end user having to enter the password for the selected Wi-Fi network on the device.
- (57) Apple shall implement an interoperability solution that provides third parties with access to the same automatic Wi-Fi connection feature described in the preceding paragraph and Section 5.8.1 of the Decision as available to Apple, in a way that is equally effective as the solution available to Apple.

- (58) Apple shall make available to third-party connected physical devices Wi-Fi Network Information saved on the end user's iOS device for Wi-Fi networks for which Apple shares such information with any of its own connected physical devices.
- (59) "Wi-Fi Network Information" consists of the information which the iOS device shares with Apple's own connected physical devices. This may include, for each Wi-Fi network: SSID (network name), indication if the SSID is broadcasted or not, the network password (if applicable), and the network security configuration. It may also include BSSID (access point identifier) and the Wi-Fi Channel number.
- (60) Apple shall provide third-party iOS companion apps with the Wi-Fi Network Information for transmission to third-party connected physical devices.
- (61) Apple shall share the Wi-Fi Network Information at the same cadence as it does for its own connected physical devices.
- (62) Apple may seek permission from the user for sharing "Wi-Fi Network Information" via a permission prompt in compliance with the requirements of Article 6(7) of Regulation (EU) 2022/1925. Among consent options that Apple offers to the user, there must be a one-time permission, so that such permission also applies to all Wi-Fi networks to which the iOS device connects in the future (provided the Wi-Fi network is in scope of paragraph (58)).¹¹
- (63) Apple shall grant third parties access to additional functionalities if necessary to enable effective interoperability with the automatic Wi-Fi connection feature referred to in paragraph (57) of this Annex.
- (64) Apple shall also provide effective interoperability with any future updates, including new functionalities, of the automatic Wi-Fi connection feature insofar as they are available to Apple's own connected physical devices. To this end, the general measures in paragraph (101) of this Annex apply, including in particular the measures concerning future updates and new functionalities set out in paragraph (101)(j) of this Annex.
- (65) Apple shall implement the measures above in compliance with the measures for all features in Section 10 of this Annex.
- (66) Apple shall implement the measures for the automatic Wi-Fi connection feature in the next major iOS release, i.e. iOS 19, and in any case by the end of 2025 at the latest. By the end of 2025, the solution must provide access to the following Wi-Fi Network Information: SSID (network name), an indication if the SSID is broadcasted or not, the network password (if applicable), and the network security configuration.
- (67) Apple shall update the solution to provide access to Wi-Fi Network Information that Apple shares with any of its own connected physical devices in the first dot release

¹¹ This measure shall not prevent Apple from showing more granular prompts, or showing prompts at a higher frequency, provided that Apple shows equivalent prompts in terms of granularity and frequency to users of its own connected physical devices. It shall also not prevent Apple from not showing any prompts with respect to third-party connected physical devices.

of iOS following 1 March 2026, i.e. iOS 19.4, and in any case by 1 June 2026 at the latest.

7. MEDIA CASTING

- (68) Apple shall provide effective interoperability with features for media casting.
- (69) The features for media casting are described in Section 5.9.1 of the Decision. The features allow Apple to provide media casting solutions, such as AirPlay, to Apple's services and hardware. Media casting is the ability to cast audio, video, and mirror screens between an iOS device and a connected physical device. Casting can take place either from an iOS device to a connected physical device, or from a connected physical device to an iOS device. Alternatively, the iOS device can be used to initiate casting between a streaming server (e.g. YouTube) and a connected physical device. In this case the iOS device connects to the connected physical device and sets up the stream, but the media stream itself takes place directly between the streaming server and the receiving device. The iOS device may act as a remote control (e.g. volume control, playback speed, etc.).
- (70) Apple shall implement an interoperability solution that provides third parties with access to the same features for media casting described in the preceding paragraph and Section 5.9.1 of the Decision as available to Apple, in a way that is equally effective as the solution available to Apple.
- (71) In particular, Apple shall allow effective interoperability with the iOS-controlled features used by Apple's media casting solutions including AirPlay. Therefore, Apple shall make the following features available to third-party casting solutions.
 - (a) Accessibility. Apple shall allow the casting solution to be selectable in the same in-app picking menu as is used for AirPlay in supported apps. The casting solution must also be selectable directly from the iOS Control Centre picker as is used for AirPlay. The end user should be able to initiate and use the casting solution without the need to open the third-party casting app in the foreground, and in the case of using the iOS Control Centre picker without the need to open the media app in the foreground.
 - (b) Centralised availability. Apple shall allow third parties to centrally provide their casting solution on iOS, e.g. through an extension, such that end users who install the casting solution can access the third-party casting provider in any app that uses standard media playback APIs without the need for the app developer to integrate an SDK in their apps.
 - (c) Advertisement and discovery. Apple shall make available device discovery that allows compatible third-party devices to be discoverable on an iOS device, enabling that the sender iOS device shows these receivers in the casting pickers in the system user interface and in apps, and make the iOS device discoverable by third-party devices, by enabling sender devices to listen for the iOS device's capabilities as a receiver.

- (d) Communication protocols. Apple shall allow third parties to make available the same communication protocols that are available to Apple's casting solutions, such as AirPlay. This includes but is not limited to Bluetooth, Infrastructure Wi-Fi, P2P Wi-Fi, and ultrawide band. Apple shall allow third parties to switch between available communication protocols and to access the required information to select the most suitable protocol. Apple shall allow third parties to integrate their media streaming protocols based on communication protocols.
 - (e) Controls. Apple shall allow the third parties to implement the same hardware button functionality (e.g. volume controls), in-app controls and lock screen controls (e.g. pause, fast forward, etc.) that are available to Apple's casting solutions, such as AirPlay.
- (72) Interoperability for third-party casting solutions must be effective. Therefore, Apple shall:
- (a) not impose limits or restrictions that may affect the audio, image or video quality achievable by third-party media casting solutions, such as inaccessibility of communication protocols, background execution restrictions, memory consumption, bandwidth limits or limits on other system resources, to the extent that these are not applied to AirPlay; and
 - (b) allow media casting solutions to use third-party DRM systems. Apple shall not impose restrictions concerning the casting of DRM-protected content that go beyond those applied to AirPlay.
- (73) Apple shall grant third parties access to additional functionalities if necessary to enable effective interoperability with the features for media casting referred to in paragraph (70) of this Annex.
- (74) Apple shall also provide effective interoperability with any future updates, including new functionalities, of the media casting features insofar as they are available to Apple's own media casting solution, such as AirPlay. For example, if Apple updates AirPlay to stream video at higher resolution, or to allow end users to initiate screen mirroring via an AI assistant, third party casting solutions should be provided the necessary interoperability to implement these functionalities as well. To this end, the general measures in paragraph (101) of this Annex apply, including in particular the measures concerning future updates and new functionalities set out in paragraph (101)(j) of this Annex.
- (75) Apple shall implement the measures above in compliance with the measures for all features in Section 10 of this Annex.
- (76) Apple shall implement the measures for the media casting features in the release of iOS 20, and in any case by the end of 2026 at the latest.

8. AUTOMATIC AUDIO SWITCHING

- (77) Apple shall provide effective interoperability with the automatic audio switching feature.

- (78) The automatic audio switching feature is described in Section 5.10.1 of the Decision. The feature allows Apple's services and hardware to implement automatic audio switching functionality via iOS with respect to Apple audio output devices. Apple's audio switching functionality allows end users using Apple's own wireless headphones to automatically have the audio source (e.g. active Bluetooth connection of a connected headset) switch between two different Apple devices, such as an iOS device and an iPad. iOS audio routing policies ensure that audio is routed to the appropriate output device, so that audio switching works according to user expectations.
- (79) Automatic audio switching on Apple devices relies on certain information from Apple and third-party apps on iOS, and from iOS. This includes the relevant audio type (e.g. media, call, notification). Relevant information also includes data and information on the current audio route, the reason for selecting the current audio source (user action, iOS decision, etc.), and information on the upcoming audio source. Automatic audio switching on Apple devices factors in signals received from Apple connected physical devices from these devices (e.g. whether Apple AirPods are currently in-ear or not).
- (80) Apple shall implement an interoperability solution that provides third parties with access to the same automatic audio switching feature described in the preceding paragraphs and Section 5.10.1 of the Decision as available to Apple, in a way that is equally effective as the solution available to Apple.
- (81) This means that Apple shall provide third parties access to the same data and information controlled or accessed by iOS that Apple uses to implement automatic audio switching functionality on Apple devices, and the ability to present their devices as a selectable audio route based on that information.
- (82) Apple shall not discriminate between its own and third-party connected physical devices in audio routing. Audio routing means iOS deciding which output channel plays audio (e.g. in-built iPhone speaker, local speakers, wired or wireless headphones) and routing audio to that channel. Apple may allow users to set audio routing preferences, but must provide such user choice in a non-discriminatory manner.
- (83) For the purpose of audio routing, Apple shall enable third parties to submit the same or similar device information to iOS and iOS must use that information in the same way as iOS uses the same or similar information from Apple connected physical devices (e.g. whether the headphone is in-ear).
- (84) Apple shall make that data and information available to third parties at the same time as it is made available to the processes or services that implement the automatic audio switching functionality on Apple devices. For instance, this concerns changes in the data and information that Apple uses to implement automatic audio switching functionality on Apple devices. To this end, the general measures in paragraph (101) of this Annex apply, including in particular the measures concerning future updates and new functionalities set out in paragraph (101)(j) of this Annex.

- (85) Apple shall grant third parties access to additional functionalities if necessary to enable effective interoperability with the automatic audio switching feature referred to in paragraphs (80) of this Annex.
- (86) Apple shall implement the measures above in compliance with the measures for all features in Section 10 of this Annex.
- (87) Apple shall implement the measures for the audio switching feature by 1 June 2026 at the latest, with exception of the functionality to present non-connected third-party devices as available audio routes. Apple shall provide effective interoperability with that functionality by 1 June 2027 at the latest.

9. NFC CONTROLLER IN READER/WRITER MODE

- (88) Apple shall provide effective interoperability with the NFC controller of iOS devices in Reader/Writer mode (“NFC Reader/Writer mode”) for third-party connected physical devices via Core NFC.
- (89) The NFC controller in Reader/Writer mode is described in Section 5.11.1 of the Decision. The NFC controller consists of a chip integrated in iOS devices, ensuring communication between an iOS device and a connected physical device via NFC technology. NFC Reader/Writer mode is an NFC mode in which an active NFC device interacts with another NFC device that acts passively. Core NFC is a publicly documented framework that allows developers to program third-party apps that can access the NFC controller of iOS devices in Reader/Writer mode to write data to NFC tags, interact with protocol-specific tags and read NFC tags, including ISO 7816 and ISO 15693, FeliCa™, MIFARE® tags and NFC tags of Types 1 to 5 that contain NDEF data. The NFC Reader/Writer mode can be used to transfer payment-related data, such as AIDs and secure credentials, including payment-related tokens. It can also be used to read smart cards, including payment cards, including to verify card possession for instance for Challenge-Response interactions.
- (90) Apple shall implement an interoperability solution that provides third parties with access to the same NFC controller in Reader/Writer mode feature described in the preceding paragraph and Section 5.11.1 of the Decision as available to Apple, in a way that is equally effective as the solution available to Apple.
- (91) To provide such access, Apple shall implement the following measures.
 - (a) Apple shall provide access to the NFC controller in Reader/Writer mode via Core NFC without AID restrictions, allowing third parties to interact with NFC devices via the NFC controller in Reader/Writer mode.
 - (b) Apple shall provide access to the NFC controller in Reader/Writer mode via Core NFC without AID restrictions, allowing third parties to transmit any APDU command referencing AIDs, in particular payment-related AIDs, from a third-party app to a connected physical device, including the SELECT command, and any data that is part of the respective APDU command, including secure credentials.

- (c) Apple shall provide access to the NFC controller in Reader/Writer mode via Core NFC to transfer secure credentials, including payment-related tokens, from the iOS device to connected physical devices.
 - (d) Apple shall provide access to the NFC controller in Reader/Writer mode via Core NFC to read smart cards, including payment cards, including to verify smart card possession, without restrictions on the deployment of third parties' security measures, such as EMV Level 2 kernels.
- (92) Apple shall grant third parties access to additional functionalities if necessary to enable effective interoperability with the NFC controller in Reader/Writer mode feature referred to in paragraph (90) of this Annex.
- (93) Apple shall also provide effective interoperability with any future updates, including new functionalities, of the NFC controller in Reader/Writer mode feature insofar as they are available to Apple's own connected physical devices. To this end, the general measures in paragraph (101) of this Annex apply, including in particular the measures concerning future updates and new functionalities set out in paragraph (101)(j) of this Annex.
- (94) Apple shall implement the measures above in compliance with the measures for all features in Section 10 of this Annex.
- (95) Apple shall implement the measures for the NFC controller in Reader/Writer mode feature in the next major iOS release, i.e. iOS 19, and in any case by the end of 2025 at the latest.

10. MEASURES FOR ALL FEATURES

- (96) According to Article 6(7) of Regulation (EU) 2022/1925, interoperability provided pursuant to Article 6(7) of that Regulation needs to be effective. This means that interoperability solutions shall be granted in a technically sound and workable manner for third parties, equally effective to the solution available to Apple, under equal conditions and without any undue obstacles. To achieve such effectiveness, Apple shall implement the measures in this section for each of the nine features referred to in Sections 1 to 9 of this Annex.
- (97) In the implementation of the specified measures, Apple may take strictly necessary and proportionate measures to ensure that interoperability does not compromise the integrity of the operating system, hardware and software features. Any integrity measure shall be duly justified and shall be based on transparent, objective, precise and non-discriminatory conditions that also apply to Apple's services and hardware. Under Article 6(7) of Regulation (EU) 2022/1925, second subparagraph, Apple shall only impose conditions and take integrity measures that reflect a genuine integrity risk and do so in a consistent and systematic manner. Under Article 6(7) of Regulation (EU) 2022/1925, second subparagraph, Apple shall only apply conditions the compliance with which is capable of being independently verified and not exclusively within the gatekeeper's control. An integrity measure cannot be considered strictly necessary and proportionate if it seeks to achieve a higher

integrity standard than the one that Apple requires or accepts in relation to its own services or hardware.

- (98) Any integrity measure shall be implemented in a way that does not undermine effective compliance with this Decision and Apple's obligations with Regulation 2022/1925 including for instance by subverting end users' or third parties' autonomy, decision-making, or free choice via the structure, design, function or manner of operation of a user interface or apart thereof.
- (99) Apple shall inform the Commission in writing of any integrity measure it intends to take, providing a justification of their strict necessity and proportionality at least 4 weeks in advance of their implementation, or without undue delay in case of urgency, unless the measure meets each of the following cumulative conditions: (i) it is not user-facing, (ii) it is exclusively of a technical nature, (iii) it is implemented for Apple and third parties in precisely the same way and (iv) Apple has determined that the change will have no or only insignificant impact of any nature on third parties, including technical or commercial impact. Apple shall retain written documentation on how any such determination was made.
- (100) Pursuant to Article 8(1) of Regulation 2022/1925, the gatekeeper shall ensure that the implementation of any measures pursuant to Article 6(7) of Regulation 2022/1925 complies with applicable law, in particular Regulation (EU) 2016/679, Directive 2002/58/EC, legislation on cybersecurity, consumer protection, product safety, as well as with the accessibility requirements.
- (101) Apple shall implement the following measures for each of the features described in Sections 1 to 9 of this Annex.
 - (a) Apple shall make available the interoperability solutions and measures implemented in compliance with this Decision to all providers of services and providers of hardware without undue delay, to the extent they indicate, including through the use of APIs, an interest in making use of any or all of the features listed in Sections 1 to 9 of this Annex.
 - (b) Apple shall not impose any restrictions on the type or use case of the software application and connected physical device that can access or make use of the features listed in Sections 1 to 9 of this Annex. Apple shall not impose any undue restrictions, including by requiring third parties to use other Apple products or services unless required for the functioning of the feature, or by requesting third parties to make choices in situations where such choice is not justified (for example, choosing between using the interoperability solution and continuing to use the same bundle ID) or prevent third parties from benefitting from access to other features, including using the feature in combination with other features within the scope of Article 6(7) of Regulation 2022/1925.
 - (c) Apple shall not undermine effective interoperability with the features listed in Sections 1 to 9 of this Annex by behaviour of a technical, commercial, contractual or any other nature. In particular, Apple shall:

- (i) enable third parties to make use of the interoperability solution in their existing apps via an automatic update of such apps; and
 - (ii) not degrade, remove, disable, or otherwise make ineffective the interoperability solution, or prevent or impede updates, including security updates, for the end user as long as the end user is eligible to benefit from the functionalities allowed by these interoperability solutions; Before taking any such measure in this respect, Apple shall notify the end user explaining how the measures Apple intends to take will affect the interoperability solution relied on by third-party services on the end user's iOS device.
- (d) Apple shall ensure that any interoperability solution implemented for the features listed in Sections 1 to 9 of this Annex is equally effective to the solution available to Apple's services and hardware, specifically Apple's own connected physical devices including, but not limited to, Apple Watch, AirPods, Apple Vision Pro, as well as any future Apple connected physical device. Apple shall apply such equal effectiveness across all dimensions, including, but not limited to, the end user journey, ease of use for end users, device and software setup, data transmission speed, and energy consumption.
- (e) To ensure access is equally effective to the solution available to Apple's own services and hardware in terms of end user journey, Apple shall not decrease the ease, convenience and speed of using third-party services and hardware from the end user perspective. In particular, Apple shall refrain from adding friction by:
 - (i) Offering choices to, or requesting permission from, the end user in a non-neutral or leading manner, including by using design patterns, dark patterns, or misrepresenting or exaggerating any risks of using the third-party connected physical device or granting a permission.
 - (ii) Preventing the third party from explaining to end users in their own language the relevance of any system prompts shown, immediately before the prompt is shown or within the prompt.
 - (iii) Showing unnecessary recurring prompts or notifications that the end user cannot easily and permanently disable in the same prompt or notification.
 - (iv) Preventing the third party from triggering a permission prompt again in the future, unless the end user has so decided.
- (f) Apple shall provide the interoperability solutions implemented to address the measures listed in Sections 1 to 9 of this Annex free of charge, irrespective of their beneficiary, application, product and use case. Apple shall also not charge any fees directly or indirectly for any of the measures set out in this Annex.
- (g) Apple shall provide complete documentation for the interoperability solution. This includes Apple making available complete, accurate and well-documented frameworks and APIs to the extent access to such frameworks or APIs are relevant for the implementation of the measures set out in this Annex.

- (h) Apple shall provide reasonable technical assistance, free of charge, to third parties to implement effective interoperability with the features listed in Sections 1 to 9 of this Annex.
- (i) Apple shall ensure that all interoperability solutions implemented to address the measures specified in this Annex are subject to Apple's usual practices, including beta testing.
- (j) Should Apple make changes to a feature listed in Sections 1 to 9 of this Annex, including with new functionalities of the feature or updates, Apple shall:
 - (i) develop such new or updated features or functionalities in a way that they are interoperable with third-party services or hardware;
 - (ii) include the interoperability solutions at an appropriate stage in the beta version of the new or updated feature or functionality;
 - (iii) make available the updated interoperability solution and documentation for the relevant feature no later than at the time the new or updated feature becomes available to any Apple's services or hardware.
- (k) Apple shall maintain the interoperability solution over time such that the solution and its documentation continue being available, functional, usable, and effective for all developers without interruption.¹² If, in exceptional circumstances, Apple wishes to deprecate an interoperability solution or parts of it, Apple shall submit a reasoned request in accordance with the procedure described in paragraph (102) of this Annex.
- (l) Apple shall communicate to the Commission within one month of the date of notification of this Decision all the measures that it intends to take to comply with the Decision in sufficient detail to enable the Commission to make a preliminary assessment as to whether the measures comply with the Decision. In particular, Apple shall: (i) describe in detail the interoperability solution it intends to make available; (ii) explain how this solution addresses all of the measures required by the Decision and will provide third parties effective interoperability under equal conditions to those available to Apple's services and hardware; and (iii) provide detailed planning of the steps leading to the implementation and release of the effective interoperability solution.
- (m) Upon expiry of the implementation deadline for each feature, Apple shall communicate to the Commission all the measures that it has taken to comply with the Decision. Under this obligation, Apple shall describe the interoperability solution made available to third parties, including all technical details and potential APIs, as well as any potential integrity measures. Apple

¹² Wherever measures in this section address maintenance or adjustment of an interoperability solution, this maintenance or adjustment covers, among others, any software changes concerning the interoperability solution. This is agnostic to the choice of how such changes are made, such as, by "refactoring" (i.e. restructuring) the existing code. This may include the creation of (and replacement by) a new framework, in the case where this is the most appropriate way of maintaining or adjusting the interoperability solution.

shall provide the Commission with a non-confidential version of this report for publication.

- (102) The Commission may, in exceptional circumstances, in response to a reasoned request from Apple showing good cause, modify or substitute one or more of the measures listed in this Annex or a part of them. The request shall not have the effect of suspending the application of the measures and, in particular, of suspending the expiry of any time period in which the measure has to be complied with.
