SECURITY, PRIVACY AND THE EUROPEAN COMMISSION'S PROPOSED IOS INTEROPERABILITY REQUIREMENTS FOR CONNECTED DEVICES UNDER THE DIGITAL MARKETS ACT

DR. IAN BROWN

2025

CTS-FGV POSITION PAPER
N. 001/2025

FGV DIREITO RIO
CENTRO DE TECNOLOGIA
E SOCIEDADE

SECURITY, PRIVACY AND THE EUROPEAN COMMISSION'S PROPOSED IOS INTEROPERABILITY REQUIREMENTS FOR CONNECTED DEVICES UNDER THE DIGITAL MARKETS ACT.

DR IAN BROWN
CTS-FGV LAW SCHOOL POSITION PAPER SERIES N. 001/2025.

This document, its results and conclusions are the sole responsibility of the author and do not represent, in any way, the institutional position of the Getulio Vargas Foundation (FGV), nor of FGV Law School Rio or the Center for Technology and Society at FGV.

ABOUT THE AUTHOR

Dr. Ian Brown is an independent researcher and consultant on Internet regulation, particularly relating to information security and privacy, digital elements of the election cycle, and pro-competitive interventions such as interoperability and data portability. He was previously Professor of Information Security and Privacy at the University of Oxford's Internet Institute, and Principal Scientific Officer at the UK Government's Department for Digital, Culture, Media and Sport. He is now a visiting professor at the Centre for Technology and Society at Fundação Getulio Vargas (FGV) Law School in Rio de Janeiro, and an ACM Distinguished Scientist. He is also a fellow of OpenForum Europe and the International University of Japan, and a member of the *Technology and Regulation* editorial board. More information is at https://www.ianbrown.tech/about/.

FUNDING

This report was commissioned by Meta Platforms Inc. as an independent expert assessment of the security, privacy and integrity implications of the European Commission's December 2024 proposals on iOS interoperability (Cases DMA.100203 and DMA.100204), where appropriate drawing out more general principles. It has been informed by 15 interviews with experts in Meta and Google, free software developers, academia, and civil society, but presents solely the author's own analysis and conclusions.

LICENSE

ACKNOWLEDGEMENTS

The author thanks the interviewees who generously shared their expertise, and colleagues who kindly reviewed drafts of the report: Alissa Cooper, Carla Florencia Griggio, Douwe Korff, Chris Marsden, Derek McAuley, Zach Meyers, Mark Nottingham, Alba Ribera Martínez and Narseo Vallina-Rodríguez. Any errors or omissions remain the author's responsibility.

ACRONYMS

API	Application Programming Interface, a way for applications to "talk" to each other and the operating system they are running on, and from there to connected devices such as smart watches, headsets, homes, cars…
AWDL	Apple Wireless Direct Link, a communications protocol based on Wi-Fi Apple uses between its own devices.
BLE	Bluetooth Low Energy, a protocol for low-powered wireless communication.
DMA	Digital Markets Act, an EU law passed in 2022.
EC	European Commission, the European Union's executive body and main enforcer of the DMA.
EDPB	European Data Protection Board, the collective body of the EU national data protection authorities plus the European Data Protection Supervisor.
ETSI	European Telecommunications Standards Institute, a body recognised in EU law for setting technical standards for its Single Market.
GDPR	General Data Protection Regulation, the EU's main law regulating the processing of personal data and protecting privacy and other fundamental rights.
GSMA	Global System for Mobile Association, a worldwide membership organisation which facilitates standards for mobile telecommunications, such as 4G/5G.
IEEE	Institute of Electrical and Electronics Engineers, a professional association which sets many key technical standards, including Wi-Fi.
iOS	Apple's iPhone operating system (OS).

IoT	Internet of Things – a common marketing term for low- or un-powered tags, cards, sensors and other simple devices which communicate with smartphones and other computing devices, using local communications protocols such as NFC and BLE.
MAC address	Medium Access Control address, a unique identifier for communications interfaces in protocols such as Wi-Fi and Bluetooth.
NFC	Near Field Communication, based on an International Organisation for Standardization (ISO) standard for unpowered payment, travel and other types of cards to wirelessly interact with payment terminals, ticket readers, iPhones, and many other devices over short distances (under 2cm), including to pair Bluetooth devices. An industry-led body, NFC Forum, brings together further related industry standards.
OS	Operating System, the computing device software which controls apps and provides them with limited access to device hardware and other resources, such as user data, as well as managing connected devices.
P2P	Peer-to-peer (for example, two devices communicating directly using Wi-Fi, rather than via an Access Point).
TLS	Transport Layer Security, an Internet Engineering Task Force standard protocol for transmitting data securely using cryptography (i.e. protecting its confidentiality and integrity).
XNU	The iOS "kernel", the high-security OS software which enforces controls on apps and connected devices' access to hardware, software and data resources.
XR	eXtended Reality devices, such as augmented or virtual reality headsets, blend a user's physical and "digital" environments.

1. EXECUTIVE SUMMARY

1.1. BACKGROUND

The EU's Digital Markets Act (DMA), passed in September 2022, contains a range of measures to improve fairness and competition in the digital sector. It requires the very largest technology companies ("gatekeepers"), such as Apple, to meet obligations in relation to their "core platform services", such as the iPhone operating system iOS. These include enabling third-party hardware and service providers to use all the features of an operating system (OS) which are available to a gatekeeper's own hardware or services (Article 6(7) DMA). This is often referred to as "vertical interoperability".

As the main DMA enforcer, the European Commission (EC) has taken a comprehensive approach to addressing iOS interoperability with connected hardware, from payment cards and virtual reality headsets to smart homes and cars. It opened an investigation into Apple's compliance in September 2024, publishing preliminary findings in December 2024 for public consultation, and specifying a range of proposed measures Apple should take (in cases DMA.100203 and DMA.100204).

The EC can take advice to ensure interoperability measures are proportionate from national and EU-wide bodies with expertise in cybersecurity (such as the EU Cybersecurity Agency) and data protection (the European Data Protection Supervisor and Board), including via the "high-level group" established under Article 40 of the DMA, as well as its own Joint Research Centre security experts. It also consults intensively with affected companies.

DMA Art. 6(7) also specifies that a gatekeeper may take "strictly necessary and proportionate" measures to protect the integrity of its OS. Recital (64) adds: "In all cases, the gatekeeper and the requesting provider should ensure that interoperability does not undermine a high level of security and data protection in line with their obligations laid down in this Regulation and applicable Union law".

1.2. DO THE EUROPEAN COMMISSION'S PROPOSED MEASURES ENABLE APPLE TO PROTECT iOS INTEGRITY AND END-USER SECURITY AND PRIVACY?

In my assessment (described fully in section 4), the EC's proposed measures are narrowly and carefully drawn to enable Apple to comply with the DMA 6(7) obligation and so provide fair and non-discriminatory iOS treatment of third-party connected devices. They are a good example of how careful, case-by-case analysis can maintain the security, privacy and integrity of a DMA-designated operating system (OS) or virtual assistant while opening related markets up to fair competition.

My assessment has been informed by interviews with 15 security and privacy experts from Meta/Google, free software developers, academia and civil society. While Apple's public response contains very limited technical detail, I refer to it where useful.

Apple's operating systems are carefully designed to reduce security, privacy and integrity risks, with a whole range of protective technical mechanisms (described in Apple's Platform Security guide). These are used to protect Apple's own services, devices and apps, and with care can also be used to enable interoperability with third-party software and devices while continuing to protect end-users.

Based on the detailed analysis described in section 3, my assessment is that the EC' s proposed measures (analysed in the table on p. 41) present lower to medium-level risks to iOS integrity and the security and privacy of iPhone users. These risks can be managed using iOS's existing technical controls, extended as appropriate (as discussed in section 3.4 and summarised in the diagram on p. 42). And as the European Commission has noted, recital 50 of the DMA can be used as further guidance:

> THE INTEGRITY OF THE HARDWARE OR THE OPERATING SYSTEM SHOULD INCLUDE ANY DESIGN OPTIONS THAT NEED TO BE IMPLEMENTED AND MAINTAINED IN ORDER FOR THE HARDWARE OR THE OPERATING SYSTEM TO BE PROTECTED AGAINST UNAUTHORISED ACCESS, BY ENSURING THAT SECURITY CONTROLS SPECIFIED FOR THE HARDWARE OR THE OPERATING SYSTEM CONCERNED CANNOT BE COMPROMISED.

Also important are legal requirements for third-party compliance with European law (such as the EU's General Data Protection Regulation (GDPR) and cybersecurity rules), discussed in section 3.5, and iOS user interface measures to ensure users provide informed permission for third-party devices to interact with specific personal data and features of their systems (discussed in section 3.4).

Apple may be required to undertake significant development to comply with some interoperability requests from third parties relating to existing iOS functionality, with a correspondingly long compliance period proposed by the EC (up to 12 months). Future iOS functionality available to Apple's own apps, devices and services must be designed to be interoperable from the start, and to comply with European data protection and cybersecurity laws.

In both cases, this functionality should be designed to be explicitly security and privacy-protective, with access to minimal iOS resources (e.g. personal data) for a specific purpose. Where this proves not to be possible, as the EC notes in its consultation (Case DMA.100203 para. 130), "Apple may take strictly necessary, proportionate and duly justified measures to ensure that interoperability does not compromise the integrity of the operating system, hardware and software features."

For one specific measured proposed by the EC (Case DMA.100203 para. 114), Apple may be justified in a more restrictive interpretation based on the data protection and cybersecurity impact. Sharing all so-called "universal" addresses of Wi-Fi Access

Points (and associated passwords) accessed previously by an iPhone with user-approved connected devices could disclose sensitive location history data, enabling user fingerprinting and profiling. iOS could limit this based on contextual factors such as recency, location, availability of more secure authentication mechanisms, and the circumstances under which the device is likely to be used separately from a paired iPhone. Imposing such limits on data transferred to connected devices (including Apple's own) would reduce the security and privacy impact of unauthorised access.

In future, gatekeepers themselves, or the EC following an investigation, might choose higher-risk technical mechanisms to enable other types of specific interoperability, alongside stronger controls to manage this risk. These controls can include existing programmes (such as Apple's MFi, and its commitments in a previous European Commission case relating to mobile payments). However, none of the EC's proposed measures in its current investigation would require such higher-risk technical changes to iOS.

My conclusion therefore is the European Commission has correctly followed the process set out in the Digital Markets Act. By carefully analysing the iOS functionality which would open the connected devices market to third parties, and through intensive consultations with interested parties and then the public, it has proposed a set of measures which would improve the fairness and contestability of this important digital market, while enabling Apple to protect the integrity of iOS and the security and privacy of its customers.

2. BACKGROUND

2.1. THE DIGITAL MARKETS ACT

The EU's Digital Markets Act (DMA), passed in September 2022, contains a range of legal measures to improve fairness and competition in the digital sector.[1] It requires the very largest technology companies ("gatekeepers"), such as Apple, to meet obligations in relation to their "core platform services", such as the iPhone operating system iOS.[2] These include enabling third-party hardware and service providers to use all the features of an OS which are available to a gatekeeper's own hardware or services (Article 6(7)). This is often referred to as "vertical interoperability".[3]

[1] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) *OJ L 265*, 12.10.2022, p. 1–66.

[2] A list of the designated "gatekeeper" firms and Core Personal Services is maintained by the European Commission at https://digital-markets-act.ec.europa.eu/gatekeepers_en

[3] See M. Borreau (Nov. 2022) *DMA Horizontal and Vertical Interoperability Obligations*, CERRE Issue Paper, at https://cerre.eu/wp-content/uploads/2022/11/DMA_HorizontalandVerticalInteroperability.pdf (although not all of the security/privacy analysis) and G. Colangelo & A. Ribera Martínez (2025) *Vertical Interoperability in Mobile Ecosystems: Will the DMA Deliver (What Competition Law Could Not)?* International Review of Law and Economics (forthcoming), at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4826150

'DMA Art. 6(7) also specifies that a gatekeeper may take "strictly necessary and proportionate" measures to protect the integrity of its OS. Recital (64) adds: "In all cases, the gatekeeper and the requesting provider should ensure that interoperability does not undermine a high level of security and data protection in line with their obligations laid down in this Regulation and applicable Union law", including the GDPR and e-Privacy Directive (ePD).

As the main DMA enforcer, the European Commission (EC) can take advice to ensure interoperability measures imposed under the Act are proportionate from national and EU-wide bodies with expertise in cybersecurity (such as the EU Cybersecurity Agency) and data protection (the European Data Protection Supervisor and Board), including via the "high-level group" established under Article 40 of the DMA, as well as its own Joint Research Centre security experts.

2.2. CONNECTED DEVICES INTEROPERABILITY

Connected hardware devices range from simple tags and sensors through to "smart" homes, cars and factories. They are a technology of central importance to Europe's near-term digital economy, and the EU's wider plans for the so-called digital and green transitions,[4] shown in the following EC illustration (Figure 1).

FIGURE 1.
SOURCE: EUROPEAN COMMISSION, EUROPE'S INTERNET OF THINGS POLICY (CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL (CC BY 4.0) LICENCE.

Interoperability between these devices and operating systems designated under the DMA will play a key role in making the markets for these devices fairer and more contestable.

2.3. THE EC INVESTIGATION INTO APPLE'S DMA ART. 6(7) COMPLIANCE

Firms designated as gatekeepers under the DMA are primarily responsible for complying with their obligations under the law. However, Apple's initial proposals for compliance were widely criticised, including for Art. 6(7), and as an academic observer noted of the public compliance workshop held by the EC in March 2024, "Apple's proposed solution is quite different to the implementation of other gatekeepers which have provided extensive interoperability solutions for particular types of services, and have not tried to obscure the process in the interim."[5]

[4] European Commission, *Europe's Internet of Things Policy*, at https://digital-strategy.ec.europa.eu/en/policies/internet-things-policy
[5] A. Ribera Martínez, *Apple's DMA Compliance Workshop – The Power of No: Breaking Apart the Bundle?* Kluwer Competition Law Blog, 19 March 2024, at https://competitionlawblog.kluwercompetitionlaw.com/2024/03/19/apples-dma-compliance-workshop-the-power-of-no-breaking-apart-the-bundle/

The EC therefore opened an investigation into Apple's Art. 6(7) compliance in September 2024, publishing preliminary findings in December 2024 for public consultation, which specified a range of proposed measures Apple should take to comply with its legal obligations in relation to iOS interoperability with third-party connected devices.[6]

2.4. THE PROPOSED EC MEASURES

This illustration (Figure 2) by Alba Ribera Martínez (included with permission) well summarises the EC's proposed connected devices measures.[7]

The measures can be grouped into three broad categories, and all apply to the extent Apple has already enabled this iOS functionality to support its own devices:

1. Allow software to run on a user's iPhone without their direct interaction, to support functionality of connected devices ("background execution").
2. Allow third-party devices to interact with existing iOS services – Apple's "Push Notification Service", AirPlay (streaming media), AirDrop (file exchange) and device-to-device Wi-Fi – and to use their own versions of AirPlay and AirDrop.

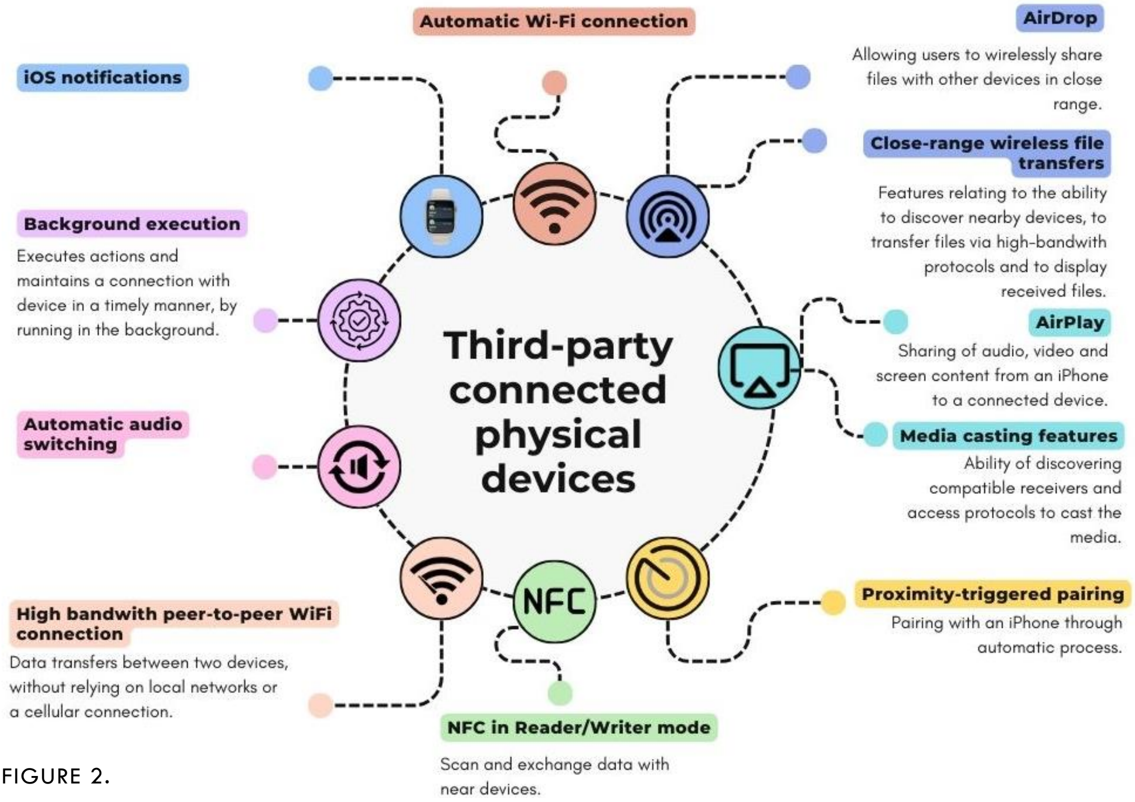

Automatic Wi-Fi connection
AirDrop
Allowing users to wirelessly share files with other devices in close range.
iOS notifications
Close-range wireless file transfers
Features relating to the ability to discover nearby devices, to transfer files via high-bandwith protocols and to display received files.
Background execution
Executes actions and maintains a connection with device in a timely manner, by running in the background.
AirPlay
Sharing of audio, video and screen content from an iPhone to a connected device.
Third-party connected physical devices
Automatic audio switching
Media casting features
Ability of discovering compatible receivers and access protocols to cast the media.
NFC
Proximity-triggered pairing
Pairing with an iPhone through automatic process.
High bandwith peer-to-peer WiFi connection
Data transfers between two devices, without relying on local networks or a cellular connection.
NFC in Reader/Writer mode
Scan and exchange data with near devices.

FIGURE 2.

[6] European Commission, *Case DMA.100203 – Consultation on the proposed measures for interoperability between Apple's iOS operating system and connected devices*, 18 December 2024, at https://digital-markets-act.ec.europa.eu/dma100203-consultation-proposed-measures-interoperability-between-apples-ios-operating-system-and_en and *Case DMA.100204 – Consultation on the proposed measures for requesting interoperability with Apple's iOS and iPadOS operating systems*, at https://digital-markets-act.ec.europa.eu/dma100204-consultation-proposed-measures-requesting-interoperability-apples-ios-and-ipados-operating_en; A. Ribera Martínez, *The Carrot of the European Commission's DMA Enforcement: Two Specification Proceedings Opened on Apple's Vertical Interoperability Integration*, Kluwer Competition Law Blog, 21 October 2024, at https://competitionlawblog.kluwercompetitionlaw.com/2024/10/21/the-carrot-of-the-european-commissions-dma-enforcement-two-specification-proceedings-opened-on-apples-vertical-interoperability-integration/

[7] *Interoperability by Design or Denial? The Digital Markets Act's Notion of Vertical Interoperability*, working paper, 2 Feb. 2025, p. 9, at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5121387

3. Give access to certain iOS-managed data, such as to enable connected headphones to switch between audio sources, or to enable devices to connect automatically to Wi-Fi Access Points.

The EC has included 15 overarching conditions Apple should meet for all its proposed measures, such as making its interoperability features openly and freely available to all competitors, with comprehensive documentation; ensuring users can grant permissions easily; and not to defeat them using contractual terms.

Apple will be required to communicate to the EC within a month "all the measures that it intends to take to comply with the decision in sufficient detail to enable the Commission to make a preliminarily assessment as to whether the measures comply with the decision." [8]

The EC has also proposed a range of alterations to the process Apple has suggested by which its competitors can request specific existing iOS features be made interoperable,[9] improving its fairness and transparency.[10]

[8] *Consultation on the proposed measures for interoperability between Apple's iOS operating system and connected devices*, footnote 6, para. 131.
[9] *Consultation on the proposed measures for requesting interoperability with Apple's iOS and iPadOS operating systems*, footnote 6.
[10] *Interoperability by Design or Denial?* Footnote 7.

3. DO THE EUROPEAN COMMISSION'S PROPOSED MEASURES ENABLE APPLE TO PROTECT IOS INTEGRITY AND END-USER SECURITY AND PRIVACY?

One of Apple's main justifications to date for not implementing many of these proposed measures has been their impact on the integrity of iOS – a justification under the DMA for limiting interoperability measures – and the security and privacy of its end-users. [11] Meta Inc. commissioned my independent assessment of the extent to which these concerns are valid.

In the following analysis, I first consider a range of relevant risks DMA Art. 6(7) interoperability measures could raise relating to OS integrity and end-user security and privacy – including those identified by Apple. Alongside the EC's proposed measures in Case DMA.100203, it has approved (with modifications) Apple's process for considering other interoperability requests in future,[12] and I therefore include some risks which should be considered at that point. The security and privacy sensitivity of such measures is summarised in the scale on p. 42.

I then consider which technical changes to iOS would be required by the EC's proposed measures, and the extent to which existing iOS security mechanisms could be applied to manage them, alongside EU legal protections such as the GDPR. This information is summarised in the table on p. 41.

As explained in section 4 below, I have assessed the integrity, privacy and security impact of the changes required by the proposed measures to be lower to medium risk, which can be dealt with using iOS security mechanisms discussed in section 3.4 and legal protections in section 3.5.

My assessment has been informed by interviews with 15 security and privacy experts from Meta/Google, free software developers, academia and civil society. While Apple's response contains very limited technical detail, I refer to it where useful.

3.1. THE IMPORTANCE OF NON-DISCRIMINATION

Apple has built its reputation for protecting user security and privacy around tight security controls within its operating systems and hardware, and the EC's proposed measures are rightly cautious about the extent to which Apple should be required to enable users to grant iOS access to third-party devices.

The DMA's Art. 6(7) non-discrimination principle is very helpful in drawing this boundary, limiting such access to the extent to which it is available to *Apple's own devices and services*. The EC's proposed measures

[11] Apple, *It's getting personal*, December 2024, at https://developer.apple.com/support/downloads/DMA-Interoperability-Dec-2024.pdf

[12] *Case DMA.100204 – Consultation on the proposed measures for requesting interoperability with Apple's iOS and iPadOS operating systems*, footnote 6.

emphasise this includes "equal effectiveness and equal conditions 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."[13]

Where Apple has given such access to its own accessories (such as AirPod wireless headphones or smart watches), this demonstrates it has already dealt with the consequent iOS-specific security and privacy risks to its own satisfaction. Where Apple has made a deliberate privacy-related decision not to collect or make available specific privacy-sensitive data, the EC's proposed measures will not require it to do so. Despite Apple's concerns, the measures would *not* provide "unfettered access to users' devices and their most personal data."[14] At most, the measures would make available to third-party devices, with explicit user consent, data and capabilities which are currently only available to Apple's own devices.

This links to psychology research on users' perception of privacy risks.[15] As one expert consulted commented: "Even when users are aware of potential data privacy risks, they may accept them if they align with the risks they consider when using (for example) Apple devices. But a notice/warning when connecting to a third-party device (e.g., for dropping a file) shouldn't be 'unfairly alarming' compared to connecting to another Apple user device."

The use and continuing development of iOS technical security controls (discussed in section 3.4 below) will enable Apple to follow the EC's proposed measures without threatening the integrity of its smartphone operating system, or the security or privacy of its users – and indeed to improve them. The company says it is already "investigating enhancements to our platform that will enable richer experiences while continuing to protect sensitive user data and maintain device security."[16]

Pre-DMA, Apple entirely decided the direction and timing of such enhancements. The DMA simply adds a mechanism for Apple's competitors to request fair and non-discriminatory treatment, overseen by the EC and ultimately the EU's courts. Apple will continue to be able to object in the case of requests which threaten iOS integrity or end-user security or privacy.

3.2. WHAT TYPES OF RISKS DOES iOS FACE WITH CONNECTED DEVICES?

A key function of computing device operating systems (supported by underlying hardware capabilities) is to control software applications and connected devices, and their access to system resources (such as user data, capabilities such as sending/receiving

[13] *Consultation on the proposed measures for interoperability between Apple's iOS operating system and connected devices*, footnote 6, para. 131(e).
[14] *It's getting personal*, footnote 11, p. 4.
[15] footnote 43.
[16] *It's getting personal*, footnote 11, p. 5.

text messages, and hardware features such as a phone's microphone or Bluetooth access). This is an essential foundation for protecting user security and privacy.

OS security controls limit the possibility of unauthorised access to those resources, whether by software or hardware vendors acting without full user consent, or malicious actors (including stalkers and domestic abusers, [17] scammers, firms conducting surreptitious user profiling, organised cybercrime gangs, and sophisticated state-level adversaries such as hostile law enforcement and intelligence agencies [18]). The EC refers to ensuring these controls continue to function as protecting the "integrity" of the OS.

As Apple notes, "Without the right protections, giving third parties access to parts of users' devices could open up ways for bad actors to steal or expose their personal information."[19] And once an iOS device has shared data with a third-party device, Apple no longer has any technical control over how it is used – although laws such as the GDPR will apply to further processing by other organisations (and in certain contexts, individuals) subject to them.

Of course, to a significant extent, these technical risks also apply to an iPhone sharing such data with an Apple device, which might also suffer from security vulnerabilities. Companies in the USA (and many other jurisdictions) are also subject to legal requirements to share user data with government authorities in certain situations.[20]

3.2.1. THE SECURITY AND PRIVACY CHALLENGES OF SYSTEM COMPLEXITY AND FRAGMENTATION

Enabling interoperability between smartphones and connected devices can pose security and privacy challenges. These can be especially significant where a smartphone OS, like Android, runs on phones supplied by multiple Original Equipment Manufacturers (OEMs). Some OEMs may be slow to push Android updates or may customise it in ways

[17] K.I. Turk & A. Hutchings, *Stop Following Me! Evaluating the malicious uses of personal item tracking devices and their anti-stalking features*. Proc. ACM European Symposium on Usable Security, Nov. 2024, at https://dl.acm.org/doi/10.1145/3688459.3688477. Relatedly, the Internet Engineering Task Force is standardising mechanisms for Detecting Unwanted Location Trackers, at https://datatracker.ietf.org/group/dult/about/

[18] Surveillance technologies and services have become a major industry, used by democracies and authoritarian governments alike. In the USA, the *New York Times* found "Immigration and Customs Enforcement, and Citizen and Immigration Services — have spent $7.8 billion on immigration technologies from 263 companies since 2020" (A. Satariano, P. Mozur, A. Krolik, and D. McCabe, *The Tech Arsenal That Could Power Trump's Immigration Crackdown*, 25 Jan. 2025, at https://www.nytimes.com/2025/01/25/technology/trump-immigration-deportation-surveillance.html). The University of Toronto's Citizen Lab has found spyware being used against democratic politicians, journalists and activists around the world (see the Lab's *Spyware Archive* at https://citizenlab.ca/tag/spyware/).

[19] *It's getting personal*, footnote 11, p. 3. Apple highlights Meta requests for access to "AirPlay, App Intents, Apple Notification Center Service, CarPlay, Connectivity to all of a user's Apple devices, Continuity Camera, Devices connected with Bluetooth, iPhone Mirroring, Messaging, Wi-Fi networks and properties". However, the EC's proposed measures cover only some of these capabilities.

[20] I. Brown and D. Korff, *Exchanges of Personal Data After the Schrems II Judgment*, European Parliament, PE 694.678, July 2021, at https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694678/IPOL_STU(2021)694678_EN.pdf

that present security or privacy risks. Google's ability to police this behaviour is limited.

As one interviewee noted, enabling iOS interoperability with connected devices (and some other, related DMA measures, such as requiring support for third-party app stores and web browser engines[21]) adds significant complexity to checking not just the security of those components, but also the security of the overall system (with all its internal and external interactions) which results. They added that in the case of the much more open Android OS, "Any [OEM] can do whatever *$&! they want and that causes a lot of security and privacy issues because it increases fragmentation."

Many Android users are also running significantly older major releases of the OS. One analysis showed only a quarter of users worldwide were using version 14, a year after its release. [22] Timely updates and patches are critical to system security.

Android's more open nature makes it significantly more flexible and customisable than iOS. But this can come with potential security and privacy consequences. Gamba *et al.* found "the supply chain around Android's open source model lacks transparency and has facilitated potentially harmful behavio[u]rs and backdoored access to sensitive data and services without user consent or awareness."[23] Dong *et al.* found "over 20,000 distinct devices operating on the Android system, featuring diverse hardware configurations," where "certain prominent device manufacturers (such as Samsung, Huawei, and Xiaomi) extensively modify the Google-led Android Open Source Project (AOSP) to appeal to a broader consumer base." Customisations may "inadvertently undermine AOSP's security protection, opening new venues for malicious actors to gain access to sensitive user information unscrupulously."[24]

Apple has its own very specific vertically-integrated business model, where it supplies the smartphone hardware (even the main "chip"/CPU and security modules) and a single OS running on it. It therefore has much greater scope to enforce security and privacy restrictions on iOS than Google does with Android – not least requiring timely software updates and carrying out security checks on apps (which Apple calls "notarisation" when it takes place outside its own App Store review process) and certain connected hardware (via its MFi programme[25]).

One expert consulted explained: "Google is aware of all these issues but has little leverage, because it can't force OEMs to

[21] *Digital Markets Act*, footnote 1, Arts. 6(4) and 5(7).
[22] Statista, *Mobile Android operating system market share worldwide from January 2018 to August 2024, by version*, at https://www.statista.com/statistics/921152/mobile-android-version-share-worldwide/
[23] J. Gamba, M. Rashed, A. Razaghpanah, J. Tapiador & N. Vallina-Rodriguez, *An Analysis of Pre-installed Android Software*, Proc. 2020 IEEE Symposium on Security and Privacy, at https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9152633
[24] Z. Dong, Y. Zhao, T. Liu, C. Wang, G. Xu, G. Xu & H. Wang, *Same app, different behaviors: Un-covering device-specific behaviors in Android apps*, arXiv preprint arXiv:2406.09807, 2024.
[25] Apple, *MFi Program – How the Program Works*, at https://mfi.apple.com/en/how-it-works

certify code as they'd go to other OSes, like Huawei's HarmonyOS" (although the ability of OEMs to do so in certain jurisdictions, including the USA, is limited).

Android's source code availability and easy configurability enables greater independent security and privacy analysis. As one expert noted: "One caveat of closed platforms is that you can't really see as clearly and easily what they are doing." While Apple provides eligible researchers with customised iPhones to carry out security research, [26] much computer science research on mobile security focuses on Android for this reason.

3.3. WHICH TECHNICAL CHANGES DO THE PROPOSED MEASURES REQUIRE IN iOS?

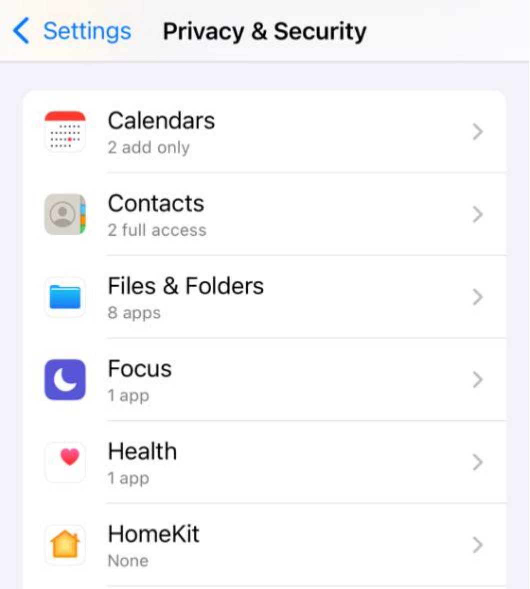
In the table shown on page 41, I have mapped the cross-cutting technical changes enabling the measures proposed by the EC[27] to be implemented on iOS to a scale of potential risks to security, privacy and integrity (colour-coded according to the table on page 42). I have also noted (in the table's second row) the iOS security controls which can be applied to manage these risks.

3.4. WHICH iOS MECHANISMS CAN BE USED TO MANAGE INTEGRITY, SECURITY AND PRIVACY RISKS?

Apple's operating systems and underlying hardware are carefully designed to reduce security, privacy and integrity risks, with a whole range of protective technical mechanisms. [28] These are used to protect Apple's own services, devices and apps, and with care can also be used to enable interoperability with third-party software and devices while continuing to protect end-users. These mechanisms include:

3.4.1. USER PROMPTS AND SETTINGS

As Apple states: "Our users deserve a complete and transparent understanding of why a developer wants access to important



Calendars
2 add only

Contacts
2 full access

Files & Folders
8 apps

Focus
1 app

Health
1 app

HomeKit
None

FIGURE 3.

[26] Apple Security Research Device Program, at https://security.apple.com/research-device

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

[28] Apple, *Apple Platform Guide*, at https://help.apple.com/pdf/security/en_GB/apple-platform-security-guide-b.pdf

parts of their devices, what that developer will do with it, and when it's happening." One specific example it provides is the iPhone microphone: "Developers must ask users for their permission to access the microphone, and they must tell users when they are using that access to record audio."[29]

The iOS functionality which enables this understanding to be provided – such as user prompts before the OS grants access to specific resources to an app, alongside detailed user-controlled settings (Figure 3) – is equally possible to apply to Apple and third parties' products and services when they are set up or configured on the user's iPhone. Apple already provides many of these OS-wide "frameworks" for apps to request access to resources, such as user calendars and address books. But as the EC importantly notes:

> AN INTEGRITY MEASURE PURSUANT TO ARTICLE 6(7) SECOND SUBPARAGRAPH OF REGULATION (EU) 2022/1925 CANNOT BE CONSIDERED STRICTLY NECESSARY AND PROPORTIONATE IF IT SEEKS TO ACHIEVE A HIGHER LEVEL OF INTEGRITY THAN THE ONE THAT APPLE REQUIRES OR ACCEPTS IN RELATION TO ITS OWN SERVICES OR HARDWARE. (SUB-PARA. 131(E))

These frameworks can be effective, in some cases, in providing users transparency into and control over access to parts of their devices. But it is important that they are tested to ensure that they are in fact providing users with transparency and control, since:

- Users may have limited time and ability to process and fully understand the consequences of their decisions.
- Norms may familiarise users with granting a higher level of permissions than they find comfortable, so legal protections remain important.

3.4.2. THE EFFECTIVENESS OF SECURITY AND PRIVACY USER NOTIFICATIONS

User configuration options can never be a security and privacy panacea. Individual users have limited time and attention to pay to these user interface features, and expertise to understand their full consequences. Even the much smaller screen size of smartphones compared to personal computers makes it more difficult to convey information, while many connected devices lack their own user interface, and can affect the privacy of everyone in a physical space – not just the owner.

A range of computer security research has examined the effectiveness of security warnings to users. An early study found "users continued through a tenth of Mozilla Firefox's malware and phishing warnings, a quarter of Google Chrome's malware and phishing warnings, and a third of Mozilla Firefox's SSL warnings."[30] A follow-up study

[29] *It's getting personal*, footnote 11, p. 2.

[30] D. Akhawe & A.P. Felt, *Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness*, Proc. 22nd USENIX Security Symposium, at https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_akhawe.pdf

"ultimately failed at our goal of a well-understood warning. However, nearly 30% more total users chose to remain safe after seeing our warning."[31] Later work found "improvements in warning design have raised adherence rates, but they could still be higher. And prior work suggests many people still do not understand them", concluding "further improvements to warnings will require solving a range of smaller contextual misunderstandings."[32]

On website identification, browser displays relating to one technical measure (HTTPS Extended Validation certificates) were found to have little effect.[33] Even the padlock icon commonly shown by web browsers to indicate connection security "is still misunderstood by many users… to indicate the general privacy, security, and trustworthiness of a website."[34] Apple's own App Tracking Transparency framework, which asks iOS users whether specific third-party apps should be allowed to track their activity across other companies' apps and websites, has been found in one study to be misunderstood by 43% of 312 participants, "including nearly a quarter who mistakenly believed that accepting a tracking request would share their location with the requesting app."[35]

That said, behavioural economics research has found that giving individuals a genuine feeling of control over their data increases their willingness to share it,[36] which gives connected device manufacturers an incentive to take measures to achieve it, alongside their obvious interest in building consumer confidence in their products. And there is promising research on ways to better convey privacy-relevant information to users, some building on existing iOS mechanisms.

Zhang *et al.* improved users' ability to understand iOS app privacy labels,[37] while Balash *et al.* studied "enhancing privacy label transparency, the importance of label clarity and accuracy, and how labels can impact consumer choice when suitable alternative

[31] A.P. Felt, A. Ainslie, R.W. Reeder, S. Consolvo, S. Thyagaraja, A. Bettes, H. Harris & J. Grimes, *Improving SSL Warnings: Comprehension and Adherence*, Proc. CHI '15, at https://dl.acm.org/doi/pdf/10.1145/2702123.2702442

[32] R.W. Reeder, A.P. Felt, S. Consolvo, N. Malkin, C. Thompson & S. Edelman, *An Experience Sampling Study of User Reactions to Browser Warnings in the Field*, Proc. CHI '18, at https://dl.acm.org/doi/pdf/10.1145/3173574.3174086

[33] C. Thompson, M. Shelton, E. Stark, M. Walker, E. Schechter & A.P. Felt, *The Web's Identity Crisis: Understanding the Effectiveness of Website Identity Indicators*, Proc. 28th USENIX Security Symposium, 2019, at https://www.usenix.org/system/files/sec19-thompson.pdf

[34] E. von Zezschwitz, S. Chen & E. Stark, *"It Builds Trust with the Customers" - Exploring User Perceptions of the Padlock Icon in Browser UI*, Proc. IEEE Security and Privacy Workshops, 2022, at https://ieeexplore.ieee.org/abstract/document/9833869

[35] H.J. Hutton & D.A. Ellis, *Exploring User Motivations Behind iOS App Tracking Transparency Decisions*, Proc. CHI '23, at https://dl.acm.org/doi/10.1145/3544548.3580654

[36] I. Brown, *The Economics of Privacy, Data Protection and Surveillance*, In M. Latzer and J.M. Bauer (eds.) *Handbook on the Economics of the Internet*, Cheltenham: Edward Elgar, 2016, pp. 247—261.

[37] S. Zhang, L. Klucinec, K. Norton, N. Sadeh, and L. F. Cranor, *Exploring Expandable-Grid Designs to Make iOS App Privacy Labels More Usable*, Proc. SOUPS '24, pp. 139–157, at https://www.usenix.org/conference/soups2024/presentation/zhang

apps are available."[38] The US government is developing a "Cyber Trust Mark" for IoT devices, and an evaluation study found "[p]articipants favo[u]red and correctly utilized the two higher-complexity labels, showing a special interest in the privacy-relevant content."[39]

A survey of 464 users of so-called eXtended Reality (XR) devices (such as smart glasses or virtual reality headsets) found "a need to enhance users' awareness of data privacy threats in XR, design privacy-choice interfaces tailored to XR environments, and develop transparent XR data practices."[40] To do so, one study developed a permission control system which enabled users to "experience the varying impacts of permission levels on not only a) privacy, but also b) application functionality… [which] allows for making better informed privacy decisions". Participants "deemed it more transparent and trustworthy than state-of-the-art [Augmented Reality] and smartphone permission systems taken from Android and iOS."[41]

Greater user control may not however always enhance privacy protection: while "users do want more control over how their information is collected and used… the feeling of security conveyed by the provision of fine-grained privacy controls may lower concerns regarding the actual accessibility and usability of information, driving those provided with such protections to reveal more sensitive information to a larger audience."[42]

More recent research has found "the intention to use privacy-invasive apps seems to be driven by whether the invasive data practices align with people's routine experiences with the data practices of typical real-world apps"[43] – so overall privacy baselines are key. Data protection law (and its effective enforcement) will remain an important mechanism for protecting users' rights, as discussed further in section 3.5 below.

3.4.3. LIMITING ACCESS TO SPECIFIC DATA ITEMS

Over the last several major versions of iOS, Apple has been adding capabilities for users to limit app access to certain categories of data to specific items, using user interface tools built into the OS – for example, files,

[38] D.G. Balash, M.M. Ali, C. Kanich, and A.J. Aviv, *"I would not install an app with this label": Privacy Label Impact on Risk Perception and Willingness to Install iOS Apps*, Proc. SOUPS '24, pp. 413–432, at https://www.usenix.org/conference/soups2024/presentation/balash

[39] C.C. Chen, D. Shu, H. Ravishankar, X. Li, Y. Agarwal & L.F. Cranor, *Is a Trustmark and QR Code Enough? The Effect of IoT Security and Privacy Label Information Complexity on Consumer Comprehension and Behavior*, Proc. CHI '24, at https://dl.acm.org/doi/10.1145/3613904.3642011

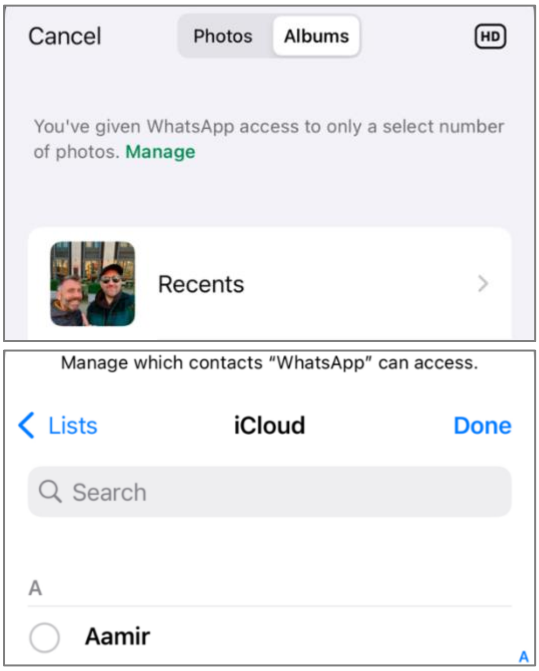
[40] H. Hadan, D.M. Wang, L.E. Nacke & L. Zhang-Kennedy, *Privacy in Immersive Extended Reality: Exploring User Perceptions, Concerns, and Coping Strategies*, Proc. CHI '24, at https://dl.acm.org/doi/10.1145/3613904.3642104

[41] M. Abraham, M. Mcgill & M. Khamis, *What You Experience is What We Collect: User Experience Based Fine-Grained Permissions for Everyday Augmented Reality*, Proc. CHI '24, at https://dl.acm.org/doi/10.1145/3613904.3642668

[42] L. Brandimarte, A. Acquisti & G. Loewenstein, *Misplaced confidences: privacy and the control paradox*, Social Psychological and Personality Science 4(3), 2013, p. 346.

[43] J.S. Seberger, I. Shklovski, E. Swiatek, and S. Patil, *Still Creepy After All These Years: The Normalization of Affective Discomfort in App Use*, Proc. CHI '22, at https://dl.acm.org/doi/10.1145/3491102.3502112

photos, and most recently contacts, as shown in these screenshots (Figure 4):



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

Manage which contacts "WhatsApp" can access.

FIGURE 4.

Where an interoperability measure requires third-party apps or connected devices are given access to resources or data managed by iOS, it would be possible for Apple to provide selective, user-controlled access using similar tools, configured on the user's iPhone, if similar restrictions could also be applied by users to Apple's own products and services.

It would be important for these tools to support users in gaining a genuine understanding of what information they were sharing. One expert gave the example that "all pictures for six months, versus all pictures ever, does not make a huge difference in terms of sensitivity" (i.e. the amount of personal information revealed).

If broad access to a rich media type (e.g. to all photos) is granted by a user, this can reveal information which might not be obvious at first glance (including location metadata if not explicitly excluded, or recognisable people or objects [44]). The implementation of the measures "are subject to Apple's usual practices, including beta testing"[45] – which clearly should include user testing.

As the EC notes, Apple should not use these or similar user interface mechanisms to "add friction that end users of Apple services and Apple connected physical devices are not subject to" – including by using "non-neutral" warnings, system defaults, time-consuming interactions, "misrepresenting any risks", or "using deceptive design pattern or dark patterns that steers users to not grant a permission."[46]

3.4.4. REQUIRING REASONS FOR API ACCESS

A related example is app access (via an API) to system data which can be used to identify (or "fingerprint") a device or user across apps from different developers (usually to "profile" an individual for the purposes of targeted advertising) – for example, the

[44] One recent security investigation found "[18] Android and [10] iOS apps on the Google Play Store and Apple App Store contain a malicious software development kit (SDK) designed to steal cryptocurrency wallet recovery phrases using optical character recognition (OCR) stealers… to extract text from [photos] on the device". B. Toulas, *Crypto-stealing apps found in Apple App Store for the first time*, BleepingComputer, 4 Feb. 2025, at https://www.bleepingcomputer.com/news/mobile/crypto-stealing-apps-found-in-apple-app-store-for-the-first-time/. Kaspersky has detailed information on the investigation at https://www.kaspersky.com/blog/ios-android-ocr-stealer-sparkcat/52980/

[45] *Consultation on the proposed measures for interoperability between Apple's iOS operating system and connected devices*, footnote 6, sub-para. 131(k).

[46] *Ibid.* sub-para. 131(f).

precise time a device was last powered up or restarted ("system boot time"). Before doing this, an iOS app must explain the reason for doing so in a "privacy manifest".[47]

3.4.5. RESTRICTING FILE-SHARING ACCESS TO CONTACTS

Relatedly, the EC's proposed measures require Apple to enable AirDrop-like services to allow users to set connections to be available to "Everyone" and "Contacts only". The measures also require "third-party connected physical devices should be able to identify nearby Apple devices as mutual contacts and vice versa".[48]

Apple has already developed a privacy-protective mechanism for doing this (based on converting contact's e-mail addresses and phone numbers into "short identity hashes" using an irreversible mathematical "hash" function)[49], although it may wish to develop this further once third-party apps and devices have broader access to this data.

3.4.6. PROTECTING SENSITIVE DATA WITH A HARDWARE-BASED SECURE ENCLAVE

Very sensitive user data – such as cryptographic keys and biometric templates used to authenticate an individual – can be processed in dedicated hardware in an iPhone, called the Secure Enclave,[50] "where not even Apple can access it."[51] For example, a specific Touch ID API lets an app check a user's fingerprint template data has been verified via the iPhone, without Apple or any other developer accessing it – "so developers of banking apps, gaming apps and more can use this technology while preserving security and privacy of the user."[52]

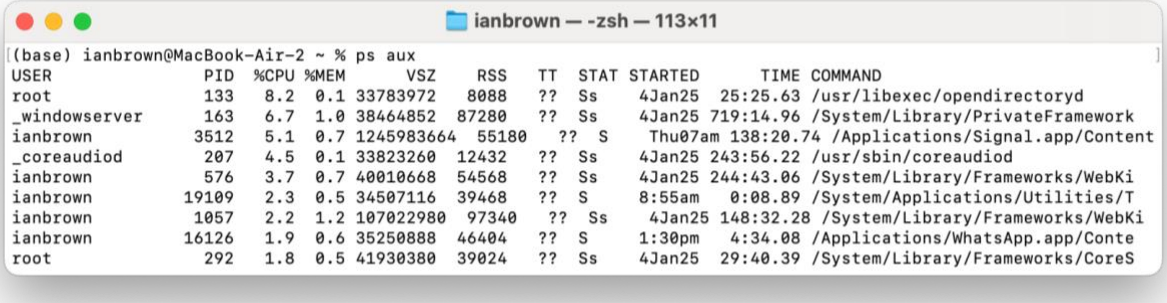
It is possible for Apple to take this type of approach with other extremely sensitive data and other system resources – as it is already doing with certain payment-related functionality. There, the company has committed to enable third-party service access to payment APIs and the iPhone's hardware Near Field Communication (NFC) sensor (to interact with standard wireless payment and other types of physical cards) to settle an antitrust case by the EC.[53]

Similarly, connected devices approved by a user could send an API request to the user's iPhone for verification and execution.

3.4.7. LIMITING BACKGROUND EXECUTION

Apple has explained iOS includes "special-purpose" mechanisms for apps to perform very specific functions while they are not

[47] Apple, *Describing use of required reason API*, Developer Documentation, at https://developer.apple.com/documentation/bundleresources/describing-use-of-required-reason-api
[48] *Ibid.* paras. 83(e) and 57.
[49] *Apple Platform Guide*, footnote 28, p. 190.
[50] *Apple Platform Guide*, footnote 28, p. 9.
[51] *It's getting personal*, footnote 11, p. 2.
[52] *Ibid.*
[53] Apple, Case AT.40452 – Mobile Payments, *Proposal of Commitments to the European Commission*, at https://ec.europa.eu/competition/antitrust/cases1/202428/AT_40452_10155330_9978_4.pdf



```
(base) ianbrown@MacBook-Air-2 ~ % ps aux
USER               PID  %CPU %MEM      VSZ    RSS   TT  STAT STARTED      TIME COMMAND
root               133   8.2  0.1 33783972   8088   ??  Ss    4Jan25  25:25.63 /usr/libexec/opendirectoryd
_windowserver      163   6.7  1.0 38464852  87280   ??  Ss    4Jan25 719:14.96 /System/Library/PrivateFramework
ianbrown          3512   5.1  0.7 1245983664  55180   ??  S     Thu07am 138:20.74 /Applications/Signal.app/Content
_coreaudiod        207   4.5  0.1 33823260  12432   ??  Ss    4Jan25 243:56.22 /usr/sbin/coreaudiod
ianbrown           576   3.7  0.7 40010668  54568   ??  Ss    4Jan25 244:43.06 /System/Library/Frameworks/WebKi
ianbrown         19109   2.3  0.5 34507116  39468   ??  S     8:55am   0:08.89 /System/Applications/Utilities/T
ianbrown          1057   2.2  1.2 107022980  97340   ??  Ss    4Jan25 148:32.28 /System/Library/Frameworks/WebKi
ianbrown         16126   1.9  0.6 35250888  46404   ??  S     1:30pm   4:34.08 /Applications/WhatsApp.app/Conte
root               292   1.8  0.5 41930380  39024   ??  Ss    4Jan25  29:40.39 /System/Library/Frameworks/CoreS
```

FIGURE 5.

currently running in the foreground (interacting with the user), such as to play audio or video, or check whether a timer has expired [54] – although one developer interviewee explained that where an app uses this functionality but is not frequently accessed by a user, the background functionality is executed less and less often by iOS, causing problems for apps relying on it to – for example – synchronise a photo collection with cloud storage.[55]

A second developer commented: "iOS actually provides background execution time to our apps on a fairly liberal basis, though the quality of background execution is often inconsistent and unreliable." In particular, "Apple's developer relations team suggests creating a notification and handling its firing, a workaround that assumes that the app is relaunched for that purpose, which it generally is not."

This type of special-purpose background functionality could possibly be extended to the specific new background capabilities required by the EC's proposed measures but would need extensive testing to ensure it was provided on a non-discriminatory basis.

Alternatively, Apple could enable background execution more generally for third-party "iOS companion apps, iOS sister applications, and relevant iOS processes"[56] – as is the norm in other operating systems, with appropriate controls, although this can have a significant impact on power consumption.

The iOS kernel ("XNU"), which controls the execution of such background processes, includes standard Unix controls on their priority, resource use and execution time. These can be partly seen in the output of the "ps" command shown below, such as the percentage of processor (CPU) and memory in use by each process. The kernel can pause and terminate errant processes at any time, including if they are rapidly draining the phone battery through outsized power consumption.

[54] Discussed in an Apple developer support post, iOS Background Execution Limits (created July 2021 by "Quinn "The Eskimo!" @ Developer Technical Support @ Apple", last updated 21 March 2024).
[55] This issue ultimately forced the UK government in 2020 to abandon its attempts to build its own Covid-19 contact tracing app, and switch to using the specific infection notification API jointly developed by Apple and Google. See I. Brown, *Regulating Privacy and Data Ethics in the Context of the UK's Contact-Tracing Apps*, in M. Hu (ed.), *Pandemic Surveillance* (London: Edward Elgar, 2022).
[56] *Consultation on the proposed measures for interoperability between Apple's iOS operating system and connected devices*, footnote 6, sub-para. 15(a).

One expert commented: "this is an area where more transparency could go a long way. Right now, people struggle to connect a dwindling battery with apps running in the background. Background execution seems like an area where there should be more transparency to the user across the board, whether for on-device or connected-device apps."

3.4.8. LIMITING CODE TO USER-SPACE

Apple has been moving towards a (much) more secure model of OS execution of code to interact with hardware devices ("device drivers"), with most such code now running (like applications) in the controlled "user-space" of the OS, rather than the (much less controlled) kernel – visualised by Wikipedia[57] as follows:

User mode	Application Environments Common Services DriverKit	**User Space**
KERNEL MODE	FreeBSD Filesystems, Networking, BSD Sockets, BSD Libraries, POSIX Thread Support	**XNU**
	OSFMK 7.3 Inter-Process Communication, Virtual Memory, Protected Memory, Scheduling, Pre-emptive Multitasking, Real-Time Support, Console I/O	

TABLE 1.

As Apple explains: "Developers can use frameworks, including DriverKit, EndpointSecurity and NetworkExtension, to write USB and human interface drivers, endpoint security tools (like data loss prevention or other endpoint agents), and [Virtual Private Network] and network tools, all without needing to write [kernel extensions]."[58]

The EC's proposed measures would not require Apple to allow third-party code to run in the iOS kernel.[59] And for the higher-layer protocols the EC is proposing Apple make available to third-party code (such as AirDrop, AirPlay, peer-to-peer Wi-Fi and Core NFC), this can be done using safe user-space technical interfaces (APIs).

Running networking-related code in user-space still has risks. One recent study found "Android mobile apps and third-party SDKs… abus[ing] user-space discovery protocols (e.g., UPnP and mDNS) to bypass the Android permissions that control the access to sensitive information such as the MAC address of the Wi-Fi Access Point… local network information is a valuable asset

[57] *The XNU Kernel Graphic*, Wikipedia, at https://en.wikipedia.org/wiki/XNU#/media/File:The_XNU_Kernel_Graphic.svg

[58] *Apple Platform Guide*, footnote 28, p. 67.

[59] By contrast, Microsoft still allows certain third-party code broad capabilities to run in the Windows kernel. This was behind the worldwide IT outage caused by CrowdStrike security monitoring software in July 2024. See I. Brown, *No, EU competition policy was not responsible for global IT chaos (I & II)*, July 2024, at https://www.ianbrown.tech/2024/07/24/no-eu-competition-policy-was-not-responsible-for-global-it-chaos-ii/

for privacy-intrusive practices like household fingerprinting and cross-device tracking."[60]

3.4.9. CHECKING AND CONTAINING DATA RECEIVED VIA LOCAL FILE-SHARING SERVICES

Parsing media and other types of complex data from untrusted senders (such as to create previews of message attachments) can create system vulnerabilities even before users take any action in response, even "leading to the inability to use a device, loss of data, or a significant loss of privacy."[61]

iOS isolates untrusted data it receives via Messages and Apple Identity Services, using a service called BlastDoor.[62] It is not clear if iOS also applies this to files shared using AirDrop, but this type of functionality could be an additional protection for data received via this route, or for iOS to apply to other AirDrop-like services.

3.4.10. USING TEMPORARY IDENTIFIERS SUCH AS MAC ADDRESSES

iOS communications protocols including Wi-Fi and Bluetooth support the use of temporary "local" communications interface identifiers, to reduce the possibility of third parties tracking iOS devices over time. [63] This functionality has become widely used, and standards bodies such as IEEE are actively developing it further. [64] It could also be supported for third-party devices connecting to iOS peer-to-peer Wi-Fi, and in AirDrop-like services.

3.4.11. SUPPORT FOR TRANSPORT LAYER SECURITY ENCRYPTION OF COMMUNICATIONS

iOS supports the latest versions of communications security protocols such as Transport Layer Security (TLS), which use cryptographic techniques (such as encryption and digital signatures) to protect the confidentiality and integrity of data sent over a channel. These protocols could protect

[60] A. Girish, T. Hu, V. Prakash, D.J. Dubois, S. Matic, D.Y. Huang, S. Egelman, J. Reardon, J. Tapiador, D. Choffnes and N. Vallina-Rodriguez, *In the Room Where It Happens: Characterizing Local Communication and Threats in Smart Homes*, Proc. 2023 ACM Internet Measurement Conference, at https://dspace.networks.imdea.org/bitstream/handle/20.500.12761/1746/IMC-181-accepted.pdf?sequence=1&isAllowed=y

[61] W.R. Vasquez Rivas, *Securing Media Parsing Code*, PhD dissertation, The University of Texas at Austin, August 2024, p. 7, at https://repositories.lib.utexas.edu/server/api/core/bitstreams/4a55a6c8-07fd-4b55-a58e-12160467ada4/content

[62] *Apple Platform Security*, footnote 50, p. 59.

[63] As E. Rye & D. Levin explain, in a 48-bit MAC address, "the second lowest order bit of the first byte—the so-called Universal/Local (U/L) bit—indicates whether the MAC address is globally assigned to a manufacturer by the IEEE (when the bit is unset), or if the MAC address is locally assigned by the device." *Surveilling the Masses with Wi-Fi-Based Positioning Systems*, Proc. 2024 IEEE Symposium on Security and Privacy, p.2, at https://www.cs.umd.edu/~dml/papers/wifi-surveillance-sp24.pdf. For the broader issues, see P. O'Hanlon, J. Wright & I. Brown, *Privacy at the link layer*, W3C/IAB workshop on Strengthening the Internet Against Pervasive Monitoring, 2014, at https://www.w3.org/2014/strint/papers/35.pdf

[64] See IEEE working group P802.11bi, *Standard for Information Technology--Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment: Enhanced Service with Data Privacy Protection*, at https://standards.ieee.org/ieee/802.11bi/10526/

third-party device communications using peer-to-peer Wi-Fi, and other types of local and remote networking links.

Correct implementation of this functionality is security-critical for communications. A review found changes to Android's equivalent TLS code by Original Equipment Manufacturers (OEMs) of mobile phones "exposes user-space apps to multiple network threats, including in/on-path intercepting proxies and surveillance if unaware app developers do not handle API inconsistencies correctly".[65] Even a security certification programme by Google "may be insufficient to prevent issues regarding API inconsistency, adherence to upstream changes, root store management, and other compliance requirements, measuring the prevalence of certain violations".[66] OEM customisations were found to "introduce TLS API fragmentation and inconsistencies that could cause user-installed apps [to] raise exceptions, behave unpredictably, or crash."[67]

However, while Android OEMs can modify lower levels of the software stack to undermine security and privacy, Apple does not face the same issue on iOS.

3.5. KEY EU LEGAL PROTECTIONS FOR END-USERS

Apple may be required to undertake significant development to comply with some interoperability requests for existing iOS functionality,[68] with a correspondingly long compliance period (up to 12 months).[69] Future functionality developed in iOS available to Apple's services must be designed to be interoperable from the start and must also comply with European data protection and cybersecurity laws (alongside "consumer protection, product safety, as well as… accessibility requirements."[70])

These laws also apply to other firms offering products and services on EU markets (including connected devices). The GDPR goes further: it applies to any personal data processing activities of organisations established within the EU (Art. 3(1)), and to those processing personal data about EU residents, even if they are not established within the bloc, if it relates to "the offering of goods or services" (Art. 3(2)(a)) or "the monitoring of their behaviour… within the Union" (Art. 3(2)(b)). The latter ("monitoring

[65] V. Bandara, S. Pletinckx, I. Grishchenko, C. Kruegel, G. Vigna, J. Tapiador and N. Vallina-Rodriguez, *Beneath the Surface: An Analysis of OEM Customizations on the Android TLS Protocol Stack*, forthcoming (copy on file with author), p. 1.
[66] *Ibid.*, p. 2.
[67] *Ibid.*, p. 10.
[68] Case DMA.100204, *Consultation on the proposed measures for requesting interoperability with Apple's iOS and iPadOS operating systems*, footnote 6, para. 55.
[69] The deadline for the EC's proposed measures is generally "in the next major iOS release, and in any case by the end of 2025 at the latest." See paras. 11, 18, 28, 42, 62, 92, 101, 110 and 120. Para. 63 states timing is confidential for "contacts mode" AirDrop support. Para. 77 gives 12 months to implement AirPlay "sender" functionality. Para. 128 gives a shorter deadline for NFC support, "in the first iOS release (minor or 'dot' release or major release) that is released three months after the date of notification of this Decision, and in any case by the end of 2025 at the latest."
[70] *Digital Markets Act*, footnote 1, Art. 8(1).

of behaviour") includes any form of online tracking and profiling.

Apple (and other designated gatekeepers) have so far chosen to offer many aspects of DMA-mandated functionality only to EU residents.[71]

3.5.1. GDPR AND E-PRIVACY DIRECTIVE (EPD)

The DMA requires that interoperability for both existing and future iOS functionality should be designed to be explicitly security and privacy-protective, with access to minimal resources (e.g. personal data) needed for a specific purpose, if it is to be used by "data controllers" to process EU residents' personal data. [72] This includes Apple as a cloud service provider. The ePD "particularises and complement[s]" the GDPR's rules for providers of electronic communications services over public communications networks to a finite number of parties (Art. 1(2)).[73]

Personal data must be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')" (GDPR Art. 1(f)). Similarly, the ePD requires an affected provider to "take appropriate technical and organisational measures to safeguard security of its services" (ePD Art. 4(1)), which at a minimum:

- ensure that personal data can be accessed only by authorised personnel for legally authorised purposes,
- protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure, and,
- ensure the implementation of a security policy with respect to the processing of personal data (Art. 4(1a)).

Organisations (and individuals, outside a "a purely personal or household activity") using personal data and subject to the GDPR, as data controllers, must "implement appropriate technical and organisational measures… designed to implement data-protection principles" by design and default (Art. 25(1)). This has been a GDPR requirement since 2018, and indeed to a significant extent of its 1995 predecessor the Data Protection Directive (Art. 17).

Specific privacy provisions also apply to the electronic communications sector under the ePD, including to service usage (Art. 6) and other location data (Art. 9), and require notification of data breaches to likely-

[71] A. Johnson, *European iPhones are more fun now*, The Verge, 25 Aug. 2024, at https://www.theverge.com/2024/8/24/24226946/iphone-eu-regulation-app-stores-fortnite
[72] An example of such a protocol is described in I. Brown, *Operating Systems need privacy-protective friend-finding services*, 4 October 2024, at https://www.ianbrown.tech/2024/10/04/2074/
[73] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) *OJ L 201*, 31.07.2002 pp. 37—47.

affected individuals and data protection authorities (ePD Art. 4(3)).

In relation to transfers of personal data to non-EU/EEA countries that have not been held by the EU to provide "adequate" protection to personal data, measures must also be taken to ensure that the authorities of those countries do not have excessive access to the transferred data, typically under law enforcement or national security laws.[74]

3.5.2. DIGITAL MARKETS ACT

Further data protection restrictions apply to companies designated as gatekeepers under the DMA, such as a prohibition on combining or cross-using data between such a firm's own core platform services with other personal data, without explicit user consent (Art. 5(2)(b) and (c)). The consent requirement is the GDPR's Art. 4(11)/7, which defines it as:

> FREELY GIVEN, SPECIFIC, INFORMED AND UNAMBIGUOUS INDICATION OF THE DATA SUBJECT'S WISHES BY WHICH HE OR SHE, BY A STATEMENT OR BY A CLEAR AFFIRMATIVE ACTION, SIGNIFIES AGREEMENT TO THE PROCESSING OF PERSONAL DATA RELATING TO HIM OR HER

The European Data Protection Board, the collective body of the EU national data protection authorities plus the European Data Protection Supervisor, has issued guidance on the meaning of consent under the GDPR. They identify key factors in determining whether consent has been "freely given". Is there an imbalance of power, such as between a government and resident, or employer and employee? Is consent required to gain access to a service where the data processing is not strictly necessary? Is the consent appropriately granular? Can the consent be withdrawn without detriment? Is consent requested for each specific purpose for the data?[75]

This DMA requirement (referring again to the GDPR) also explicitly allows processing based on a legal obligation, "to protect the vital interests of the data subject or of another natural person", or when "necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller".[76]

Meyers suggests that where a gatekeeper limits interoperability functionality for security purposes, the DMA requires assessing the proportionality of such limits to be based on "the likelihood and severity of a particular security risk occurring; the degree to which a restrictive measure… would address them; and the extent to which the measure would limit…the right of app

[74] The European Data Protection Board has clarified what it regards as not excessive access in its European Essential Guarantees for state surveillance powers. In several cases, the EU Court of Justice has held that a third country (i.e., the USA) was wrongly held to provide "adequate" protection when in fact the surveillance powers of its authorities did not meet those standards (*Schrems I* and *II*). See *Exchanges of Personal Data After the Schrems II Judgment*, footnote 20.

[75] EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679*, version 1.1, adopted on 4 May 2020, pp. 8—13, at https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

[76] *Digital Markets Act*, footnote 1, referencing GDPR Art. 6(1)(c/d/e).

developers to compete with Apple and Google by offering the same functionality."[77]

The EC's proposed measures require Apple to "describe in detail every measure it has adopted or plans to adopt to ensure that the integrity of iOS is not compromised, explaining why such measure is strictly necessary and proportionate. Apple shall provide the [European] Commission with a non-confidential version of this report for publication."[78]

3.5.3. CYBER RESILIENCE AND SECURITY ACTS

From December 2027, new cybersecurity obligations will apply to digital products (including OSes and connected devices) in the EU under the Cyber Resilience Act, including that they are "designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks."[79]

Based on a security assessment, products must be made available "without known exploitable vulnerabilities", "with a secure by default configuration" and "where applicable… [receive] automatic security updates". [80] OSes are designated as "important" products, [81] and must meet a higher standard of testing.[82]

The EU has also created a detailed legal framework for the certification of products' and services' digital security under its Cyber Security Act.[83]

[77] Z. Meyers, *Balancing security and contestability in the DMA: the case of app stores*, European Competition Journal, Apr. 2024, pp. 14-15, at https://doi.org/10.1080/17441056.2024.2340869

[78] *Consultation on the proposed measures for interoperability between Apple's iOS operating system and connected devices*, footnote 6, sub-para. 131(o).

[79] 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), *OJ L, 2024/2847*, 20.11.2024: Art. 71 and Annex I.

[80] *Ibid.*, Annex I Part I.

[81] *Ibid.*, Annex III.

[82] *Ibid.*, Art. 32.

[83] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), *OJ L 151*, 7.6.2019, p. 15–69.

4. OVERALL ASSESSMENT

Given the risks presented by the technical changes I have identified to iOS required by the EC's proposed measures, described in sections 3.2 and 3.3, my assessment is that the measures present lower to medium-level risks to iOS integrity and the security and privacy of iPhone users – as shown in the diagram on page 42. These risks can be managed using iOS's existing technical controls, extended as appropriate, as discussed in section 3.4.

Also important are legal requirements for third-party compliance with European law (such as the GDPR) discussed in section 3.5, and iOS user interface measures to ensure users understand and control how third-party devices interact with specific features of their systems (discussed in section 3.4).

From December 2027, manufacturers of connected devices placed on the EU market will have a range of obligations under the Cyber Resilience Act to maintain basic levels of cybersecurity (including automatic updates where applicable).[84] This will significantly improve the security and privacy baseline for third-party devices connecting to iOS.

As discussed in section 3.2, it will be important for Apple to continue evaluating the impact of iOS changes on overall system integrity, security and privacy. As the EC's proposed measures repeatedly note, these are important considerations in the specific changes Apple makes in response to the DMA. Recital 50 of the DMA can be used as guidance:

> THE INTEGRITY OF THE HARDWARE OR THE OPERATING SYSTEM SHOULD INCLUDE ANY DESIGN OPTIONS THAT NEED TO BE IMPLEMENTED AND MAINTAINED IN ORDER FOR THE HARDWARE OR THE OPERATING SYSTEM TO BE PROTECTED AGAINST UNAUTHORISED ACCESS, BY ENSURING THAT SECURITY CONTROLS SPECIFIED FOR THE HARDWARE OR THE OPERATING SYSTEM CONCERNED CANNOT BE COMPROMISED.

In "strictly necessary, proportionate and duly justified" circumstances, as the proposed measures allow, Apple may need to circumscribe interoperability measures to protect the integrity of iOS and its hardware and software features.[85]

Where substantial iOS changes are needed to safely support interoperability capabilities, a longer implementation process may be justifiable, up to a maximum of 12 months, as the EC measures on the process of considering interoperability requests allow.[86]

[84] See footnote 80.
[85] Case DMA.100204, *Consultation on the proposed measures for requesting interoperability with Apple's iOS and iPadOS operating systems*, footnote 6, para. 7.
[86] *Ibid.*, para. 55.

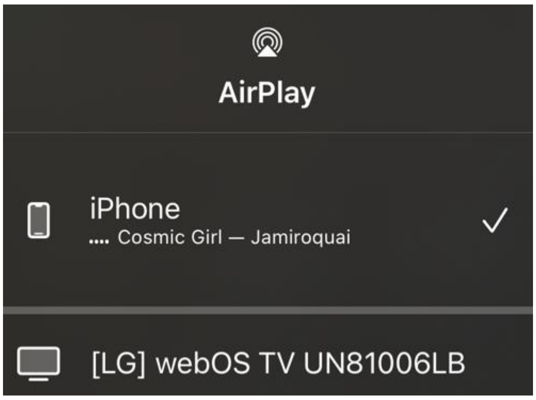
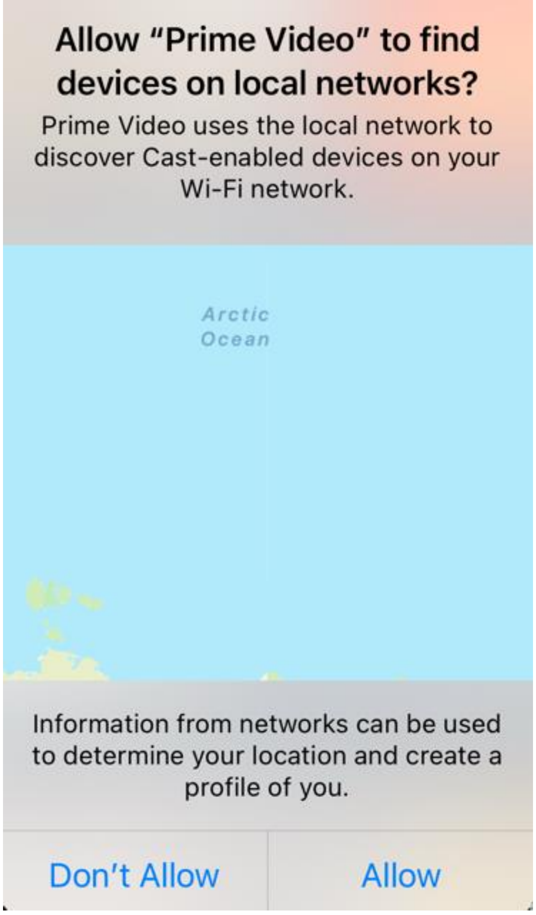


FIGURE 6.



Allow "Prime Video" to find devices on local networks?

Prime Video uses the local network to discover Cast-enabled devices on your Wi-Fi network.

Information from networks can be used to determine your location and create a profile of you.

FIGURE 7.

One technologist consulted suggested this "is not a generous period to develop [further] interoperability measures [requested by developers], even if it's all under one roof." That said, the Art. 6(7) interoperability requirements for gatekeepers have been under active debate since they were included in the EC's DMA proposal published in late 2020.

The proposed measures give Apple yet more time to comply with the law, nearly a year after it came into full applicability. Even then, the EC has proposed that:

> IN STRICTLY EXCEPTIONAL AND DULY JUSTIFIED CASES, WHERE, DESPITE HAVING TAKEN ALL NECESSARY ACTIONS TO HANDLE THE [FURTHER INTEROPERABILITY] REQUEST [FROM A DEVELOPER] IN A TIMELY MANNER – INCLUDING HAVING ADEQUATELY PRIORITISED THE HANDLING OF THE REQUEST AND MOBILISED SUFFICIENT RESOURCES TO THAT EFFECT – APPLE IS NOT ABLE TO COMPLY WITH ONE OF THE TIMELINES…APPLE SHOULD INFORM THE DEVELOPER AND NOTIFY THE COMMISSION AS EARLY AS POSSIBLE, AND SHOULD EXPLAIN IN SUFFICIENT DETAILS THE OBJECTIVE REASONS FOR SUCH DELAY. APPLE SHOULD ENSURE THAT THE DELAY IN SUCH SITUATION IS AS LIMITED AS POSSIBLE.[87]

4.1. SHARING CERTAIN DATA RATHER THAN LIMITED CAPABILITIES CAN INCREASE RISK

One important distinction to make in terms of resulting security and privacy risk is between iOS making limited capabilities available to an app – for example, to set-up and use an AirPlay connection (Figure 6) – and sharing broader data with a third-party device, with less potential control over its use.

[87] *Ibid.*, para. 67.

4.1.1. WIRELESS PROTOCOL ACCESS

Where iOS devices must be "discoverable" by connected devices – for example, for the latter to act as AirPlay senders – this means they must locally broadcast some data (e.g. using Wi-Fi or Bluetooth) which any compatible device can interpret. This is how iOS enables apps to connect to AirPlay receivers (Figure 7).

While iOS limits app access to this data, the same mechanism cannot be applied to connected devices running other operating systems. And as Girish *et al*. noted, attackers who manage to compromise a device on a home network, behind a firewall, can "exploit device vulnerabilities or local network protocols to gather privacy- or security-sensitive data from other devices in the same local network, an attack that would not be possible from the Internet."[88]

Apple is correct to note this will provide third-party devices with *some* "data about users' homes"[89] (in terms of available iOS AirPlay devices) or other environments where they are used. However, this data appears to be quite limited, and already available to connected devices in a home.[90]

It should be noted this potential for monitoring is currently a very common aspect of wireless communications protocols such as Wi-Fi. Any device with Wi-Fi access can monitor the local radio environment and information broadcast in it. Girish *et al*. found six "Internet of Things" Android apps – including Amazon's Alexa – sharing information about nearby devices they were not already connected to, to first and third-party cloud services such as "Tuya, a China-based IoT platform provider".[91] They also found "three particularly brazen cases of third-party libraries present in Android apps gathering local network information",[92] and that it was possible for tracking code to "fingerprint" individual homes based on the combination of devices detected.[93]

This suggests industry-wide responses may be needed. Partial risk mitigations include devices using frequently-changed, randomised identifiers, as discussed in section 3.4.

[88] *In the Room Where It Happens*, footnote 60.
[89] *It's getting personal*, footnote 11, p. 4.
[90] Apple does not publicly document the AirPlay protocol, but unofficial "reverse-engineered" versions of it are available. See for example *Service Discovery* in the *Unofficial AirPlay Specification*, at https://openairplay.github.io/airplay-spec/service_discovery.html
[91] *Ibid.*, s. 6.1.
[92] *Ibid.*, s. 6.2
[93] *Ibid.*, s. 6.3.

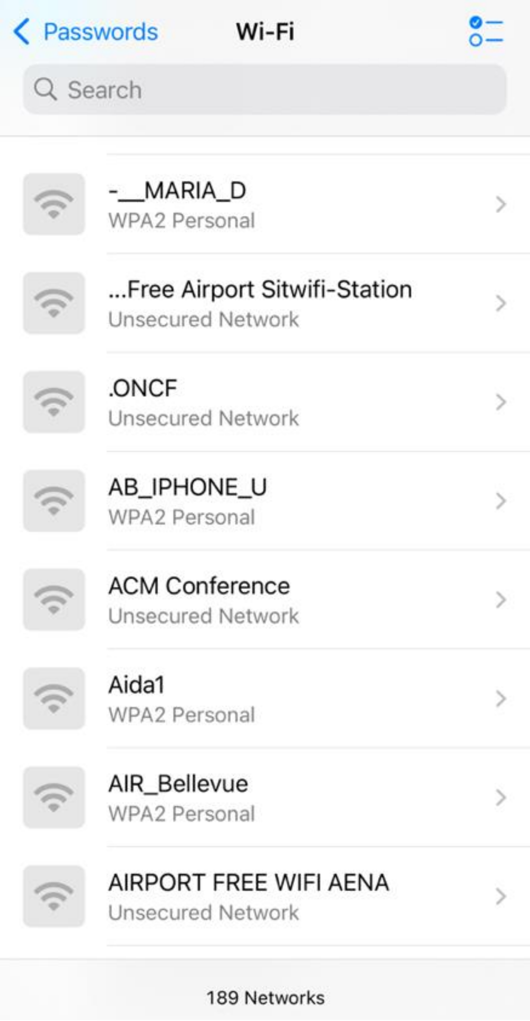
4.1.2. SHARING WI-FI ACCESS POINT DATA

The EC's proposed measures also require iOS to (continually) share information with connected third-party devices about the Wi-Fi networks the end-user has previously connected to, including security information such as passwords, to the extent this is done with Apple's devices.[94] Depending on how often individual Apple device users connect to Wi-Fi as they move around the world, this can contain a significant amount of data (Figure 8).

This information could trivially be used to look up a partial location history of the user, if universal permanent identifiers (such as the EC's proposed Wi-Fi Access Point identifier BSSID[95]) are included, given the availability of services such as Apple's Wi-Fi geolocation API and Maps.

To give just a few obvious examples, even single BSSIDs can disclose particularly privacy-sensitive location history, such an abortion or mental health clinic, gay bar, domestic violence shelter, or mosque. Lists of BSSIDs provide insight into an individual's patterns of life and enable fingerprinting, while overlaps of lists between individuals can be suggestive of overlapping group and community affiliations.

Rye and Levin further explain the vulnerabilities widespread availability of BSSID-location information can introduce if exploited at scale.[96] And as the GDPR (recital 30) notes, "Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to



< Passwords Wi-Fi

Search

-__MARIA_D
WPA2 Personal

...Free Airport Sitwifi-Station
Unsecured Network

.ONCF
Unsecured Network

AB_IPHONE_U
WPA2 Personal

ACM Conference
Unsecured Network

Aida1
WPA2 Personal

AIR_Bellevue
WPA2 Personal

AIRPORT FREE WIFI AENA
Unsecured Network

189 Networks

FIGURE 8.

[94] *Consultation on the proposed measures for interoperability between Apple's iOS operating system and connected devices*, footnote 6, para. 114.
[95] *Consultation on the proposed measures for interoperability between Apple's iOS operating system and connected devices*, footnote 6, para. 114.
[96] *Surveilling the Masses with Wi-Fi-Based Positioning Systems*, footnote 63.

create profiles of the natural persons and identify them."

A potential mitigation would be to put contextual limits on which universal Wi-Fi network data iOS shares with all connected devices, based on factors such as recency, frequency, location, sensitivity, availability of more secure authentication mechanisms, and the circumstances under which the device is likely to be used separately from a paired iPhone (which could otherwise provide specific network authentication data at the point it is needed.) I would argue this would be a justifiable data minimisation measure, provided it is implemented in a non-discriminatory way.

A broader protective measure which would better protect Apple's users (including on its own systems) would be to limit the storage and sharing of Wi-Fi data generally, based on contextual factors (such as whether the user is likely to re-visit the location in future and the potential sensitivity of the system or location). Users could also be given greater control over how long specific passwords are stored and shared (including with nearby contacts). Finally, Apple could consider limiting the availability of its geolocation service, as Rye and Levin recommend (and Google already does).[97]

Outside Apple's direct control would be to encourage the industry-wide use by Wi-Fi Access Points of privacy extensions, such as using and frequently updating randomised identifiers (BSSIDs), and to contribute to the further development of wireless communications protocol standards privacy extensions, such as IEEE's. An amendment to the Wi-Fi standard has already been proposed, "introduc[ing] mechanisms to enable session continuity in the absence of unique MAC address-to-[device] mapping. For [devices] in an [Wi-Fi network] that use randomized or changing MAC addresses, this amendment preserves the ability to provide customer support, conduct network diagnostics and troubleshooting, and detect device arrival in a trusted environment".[98]

As Meyers notes, it could save DMA enforcers significant time and resources if they can incentivise gatekeepers to take this kind of collective action towards compliance.[99]

Where manufacturers of third-party devices (or other connected service providers) process such data relating to people in the EU, they will (like Apple) need to meet GDPR requirements such as complying with the data protection principles (Article 5) and having a lawful basis (Article 6), such as consent for a specific purpose, as discussed in section 3.5.

[97] *Ibid.*, s. 9. Apple has taken some steps to reduce the amount of information revealed by its geolocation service (relating to how quickly newly-discovered Access Points are added to its database) but these have not yet been independently evaluated: Personal communication from E. Rye, 23 Jan. 2025.

[98] IEEE Approved Draft Standard for Information Technology--Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks--Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Operation with Randomized and Changing MAC Addresses, P802.11bh/D6.0, Aug 2024, at https://ieeexplore.ieee.org/servlet/opac?punumber=10630677

[99] Z. Meyers, *Which governance mechanisms for open tech platforms?* CERRE Issue Paper, Jan. 2025.

Given the potential sensitivity of such data, however, Apple would be justified in exploring limits to how it is shared with both Apple and third-party devices. This could include the development of privacy-protective APIs which, for example, limit the availability of universal permanent identifiers to connected devices, and enable such devices to connect to wireless networks using more secure techniques than shared passwords, built on existing standards such as the IEEE's 802.1X, already supported by iOS.[100]

[100] IEEE 802.1X-2020, *IEEE Standard for Local and Metropolitan Area Networks--Port-Based Network Access Control*, 28 Feb. 2020, at https://standards.ieee.org/ieee/802.1X/7345/

5. CONCLUSIONS

In my assessment, the EC's proposed measures are narrowly and carefully drawn to enable Apple to comply with the DMA Art. 6(7) obligation and so provide fair and non-discriminatory iOS treatment of third-party connected devices. They leave space for Apple to further develop its technical controls to better protect both its own and third-party connected devices, not least to comply with European data protection and cybersecurity law. This will be important where potentially sensitive iOS data (such as universal identifiers of connected Wi-Fi Access Points) are shared with connected devices. Apple will continue to need to carefully assess the overall system levels of security and privacy of its iPhones.

The proposed measures are a good example of how careful, case-by-case regulatory analysis can take proper account of the security, privacy and integrity of a DMA-designated OS (or virtual assistant) while opening related markets to fair competition. The DMA requirements for non-discriminatory treatment and compliance with EU laws such as the GDPR have proven important to this.

Apple may be required to undertake significant development to comply with further interoperability requests from third parties relating to existing iOS functionality, with a correspondingly long compliance period proposed by the EC (a maximum of 12 months). Future iOS functionality available to Apple's own apps, devices and services must be designed to be interoperable from the start, and to comply with European data protection and cybersecurity laws.

In both cases, the DMA requires this functionality should be designed to be explicitly security and privacy-protective,[101] with access to minimal iOS-managed resources (e.g. personal data) for a specific purpose (shown as "interoperability by design" in the top left of the table on p. 41). Where this proves not to be possible, as the EC notes in its consultation, "Apple may take strictly necessary, proportionate and duly justified measures to ensure that interoperability does not compromise the integrity of the operating system, hardware and software features."[102]

Apple was required by the DMA to make iOS features available to its own services and hardware interoperable by March 2024. Given it has yet to fully do so, the EC has appropriately followed the process set out in the Digital Markets Act to further specify compliance requirements.

By carefully analysing the iOS functionality which would open connected devices markets to third parties, and through intensive consultations with interested parties and then the public, the EC has proposed a set of measures which would improve the fairness and contestability of these important

[101] See Case DMA.100204, *Consultation on the proposed measures for requesting interoperability with Apple's iOS and iPadOS operating systems*, footnote 6 (especially para. 7).
[102] *Consultation on the proposed measures for interoperability between Apple's iOS operating system and connected devices*, footnote 6, para. 130.

markets, while enabling Apple to protect the integrity of iOS and the security and privacy of its customers.

5.1. FUTURE DIRECTIONS

The final decisions of the EC in these cases will send an important signal of the level of interoperability required for operating systems and virtual assistants designated under the DMA.[103] While Windows and Android (the other two currently-designated OSes) are much more open than iOS[104] (and iPadOS, which was designated on 29 April 2024[105]), the decisions will be significant for Microsoft and Alphabet as well as Apple. They will demonstrate the EC's determination for Europe's now extensive digital rulebook to be enforced, with DMA-designated OSes and virtual assistants interoperable by default, while protecting users' security and privacy.

The EC's decisions also have the potential to significantly boost the levels of innovation, investment and competition in substantial digital markets built around OSes and virtual assistants. This is equally true for both European startups and small firms, and businesses elsewhere that want to supply the EU's roughly 450m residents. These firms, and their investors, will have stronger confidence they will be able to connect innovative, trustworthy products and services to the smartphones, tablets and personal computers that for the foreseeable future will remain the hubs of the digital economy.

Many companies are likely to make future requests to Apple for interoperability relating to existing functionality which go further than the EC's proposed measures, and the EC has accepted (with modifications) Apple's proposed process to consider these.[106] It is possible to envisage other types of interoperability access which *would* threaten the integrity of an operating system, shown in the right-most sections of the table on page 41. But such measures have *not* been proposed by the EC in this case. They would have to be assessed by Apple, if requested, on a case-by-case basis.

In future, gatekeepers themselves, or the EC following an investigation, might choose higher-risk technical mechanisms to enable other types of specific interoperability, alongside stronger controls to manage this risk. These controls can include existing programmes, such as checks during Apple's notarisation and MFi certification, [107] and its NFC Entitlement

[103] It will ultimately be for the EU's courts to determine this as they interpret the DMA.

[104] Hence why, alongside Apple's apparently grudging DMA compliance, this is the first type of DMA "specification" process undertaken by the EC – even if Apple complains it is "the only company being forced to share its innovations in this way with everyone else." (*It's getting personal*, footnote 11, p.4.) Ribera Martínez commented Apple's initial proposal for broad DMA compliance faced "huge criticism on the side of developers, and Apple encountered three main trainwrecks leading towards the compliance deadline (and after it!)" (footnote 5).

[105] Apple was required to comply with its obligations related to iPadOS six months later, after the EC had opened this investigation, under DMA Art. 3(10). *Summary of Commission Decision of 29 April 2024 relating to a decision pursuant to Article 17 of Regulation (EU) 2022/1925 (C/2024/4374)*.

[106] The EC has consulted on requirements for this process in Case DMA.100204, *Consultation on the proposed measures for requesting interoperability with Apple's iOS and iPadOS operating systems*, footnote 6.

[107] *MFi Program – How the Program Works*, footnote 25.

Program in a previous EC competition case relating to mobile payments.[108]

Over time, it would be beneficial for competition if standards for security (such as those applied by Apple in its MFi and notarisation programmes) were set industry-wide and open to evaluation by third parties – for example, as is the Consumer Mobile Device Base Protection Profile developed by the European Telecommunications Standards Institute (ETSI).[109]

This standard was certified in January 2024 by the French cybersecurity agency ANSSI under the Common Criteria global certification framework,[110] and is being used as the basis of an industry-wide evaluation and certification framework for mobile device security from industry association GSMA.[111] This approach could align with the certification framework in the EU Cybersecurity Act.

Traditional standards-setting can be slow-moving,[112] so for faster-changing environments a more flexible, open governance approach may sometimes be preferable.[113] But leaving too much discretion to gatekeepers to control the process risks it being shaped to enhance their interests and even market power, rather than opening digital markets.[114] As one expert consulted noted:

> ALLOWING BIG TECH VENDORS TO DEFINE WHAT INTEROPERABILITY IS – EVEN UNDER SCRUTINY – STILL ALLOWS THEM TO DEFINE THE LANDSCAPE, AND IT'S INEVITABLE THAT THE SOLUTIONS WILL HAVE BIG-TECH-SHAPED-HOLES TO FILL IN THEM. THIS IS A PROBLEM I'M BECOMING MORE AND MORE CONCERNED ABOUT: REGULATION IS HAVING THE EFFECT OF CROWNING THE WINNERS AS KINGS WHO ARE WATCHED CLOSELY BUT STILL HAVE IMMENSE POWER, AND IT PRECLUDES THE DEVELOPMENT OF OTHER MORE HEALTHY APPROACHES.

A good example is the proposed measure's treatment of automatic audio switching. Apple's current version of this relies on devices all being logged into the same Apple account.[115] It seems unlikely Apple is going to open this account system to its competitors, and the proposed measures would not require it to do so.

Apple will be able to develop other mechanisms to meet the EC's requirements –

[108] *Proposal of Commitments to the European Commission*, footnote 53.

[109] ETSI TS 103 732-1 V2.1.2 (2023-11), at https://www.etsi.org/deliver/etsi_ts/103700_103799/10373201/02.01.02_60/ts_10373201v020102p.pdf

[110] ETSI, *ETSI Protection Profile for securing smartphones gains world-first certification from French Cybersecurity Agency*, 12 January 2024, at https://www.etsi.org/newsroom/press-releases/2308-etsi-protection-profile-for-securing-smartphones-gains-world-first-certification-from-french-cybersecurity-agency

[111] GSMA, *Mobile Device Security Certification Scheme – Overview Version 1.0*, 18 September 2024, at https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/10/FS.53-v1.0.pdf

[112] J. Baron & P. Larouche, *The European standardisation system at a crossroads*, CERRE Report, May 2023, at https://cerre.eu/publications/the-european-standardisation-system-at-a-crossroads/

[113] *Which governance mechanisms for open tech platforms?* Footnote 99.

[114] A. Ezrachi and M.E. Stucke, *The Darker Sides of Digital Platform Innovation*, Network Law Review, 2022, at https://www.networklawreview.org/ezrachi-stucke/

[115] Apple, *Switch your AirPods to another device*, at https://support.apple.com/en-us/104988

perhaps based on the hashing mechanisms it uses to identify contacts' devices in AirDrop (discussed in section 3.4). But will competitors also be able to use such mechanisms to securely enable this functionality between their own and compatible devices? If not, they will face twice the development costs of Apple – which is unfortunate, given their respective statuses as challengers and gatekeeper (a DMA problem also seen in its Art. 7 interoperability provision for messaging and conferencing tools).

Alongside addressing such issues, two significant advantages of using cross-platform international standards as the basis for interoperability mandates are its regulatory efficiency,[116] and the common security and privacy analysis it enables.[117]

For example, to enable peer-to-peer Wi-Fi, the EC proposed measures would allow Apple to make available to third-parties its own ad-hoc protocol Apple Wireless Direct Link (AWDL).[118] It would arguably be better for system security for Apple to adopt the industry-standardised Wi-Fi Aware protocol, the EC's second option,[119] which would enable greater scrutiny and testing/analysis by third parties[120] – as well as reducing the cost of cross-platform development for third-party app and connected device creators. It does however seem in this case that Apple has displayed greater agility in addressing vulnerabilities, which is easier when updates do not require agreement with other parties for a standards-based equivalent.

Similarly, if Apple makes more information publicly available about its AirPlay specification (discussed in s. 4.1) this will enable greater independent security and privacy analysis of it. This would be reinforced if over time it was standardised and used cross-industry.

[116] I. Brown and C. Marsden, *Interoperability as a standard-based ICT competition remedy*, 2013 8th IEEE International Conference on Standardization and Innovation in Information Technology, at https://doi.org/10.1109/SIIT.2013.6774570

[117] It would be a reasonable hypothesis that security and privacy analysis complexity grows faster than linearly with additional protocols to check, given their potential cross-interactions.

[118] *Consultation on the proposed measures for interoperability between Apple's iOS operating system and connected devices*, footnote 6, para. 36.

[119] *Ibid.*, para. 38.

[120] Vulnerabilities were found in Wi-Fi Aware in 2021: L. Almon, A. M. Krause, O. Fietze, and M. Hollick, *Desynchronization and MitM Attacks Against Neighbor Awareness Networking Using OpenNAN*, in Proc. MobiWac '21, pp. 97–105, at https://dl.acm.org/doi/10.1145/3479241.3486689. In a personal communication on 4 Feb. 2025, the lead author confirmed: "To the best of my knowledge the issues never got addressed. Which is a pity, since the protocol itself has great potential to build decentralized ad-hoc networks. It remains a niche area/topic." Serious vulnerabilities were found in AWDL in 2019 by an academic team (M. 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*, Proc. USENIX Security '19, pp. 37–54, at https://www.usenix.org/conference/usenixsecurity19/presentation/stute), one of which was fixed at the time, and additionally in early 2020 by a Google researcher (fixed in May 2020): I. Beer, *An iOS zero-click radio proximity exploit odyssey*, at https://googleprojectzero.blogspot.com/2020/12/an-ios-zero-click-radio-proximity.html?m=1

Jurisdictions outside the EU (including the UK[121] and Brazil[122]) have or are developing similar legal frameworks to the DMA, which include the use of interoperability to increase digital market fairness and contestability. While an *a la carte* approach enables a jurisdiction to make fine-grained choices based on its own national situation, it will make both implementation by regulated firms, and verification of the resulting security and privacy impact, significantly more difficult.

5.2. INNOVATION FOR SECURITY AND PRIVACY

As Apple has noted, "We have pioneered approaches, for both developers and ourselves, that enable amazing user experiences without any company—including Apple—gaining access to users' private data. This is the foundation for user trust, and part of what enables success for everyone: users, developers, and Apple."[123]

Space for this innovation remains under the DMA, as will the opportunity for any company to differentiate its products by going further than competitors on security and privacy protections. This is true for the DMA's core platform services (such as operating systems), and for services built on top of them. As one expert consulted said: "it doesn't affect Apple's ABILITY to innovate (except for 'innovations' that are contrary to 6(7) and are therefore likely to be anticompetitive practices masquerading as security improvements)."

One recent example is two serious hardware security flaws which affect Safari running on newer Apple processors. Other web browsers (Chrome, Firefox, Edge, Opera, and Vivaldi) have implemented a stronger version of a security mechanism termed "site isolation", which protects entirely against one flaw and significantly against the other. They are therefore better protected on Android, where they can use their own browser engines, while "Apple lags several years behind in this important protection" on iOS.[124]

But until Apple has complied with a related DMA obligation (Art. 5(7)) to allow third-party web browser engines to run on iOS, those other browsers *are* affected to the same degree as Safari on that platform. Apple was given pre-publication notification of these flaws, yet for one of them (named "SLAP") was yet to fix them 250 days later.[125]

Firms with DMA-designated OSes and virtual assistants will have to make new functionality available to their own complementary products and services available to

[121] UK Competition & Markets Authority, *Strategic Market Status investigation into Apple's mobile ecosystem*, 23 Jan. 2025, at https://www.gov.uk/cma-cases/sms-investigation-into-apples-mobile-ecosystem#case-information

[122] A. Sadami and N. Zingales, *Brazil: Ex Ante Regulation of Ecosystems, the Clash of Different Approaches and Paths Forward*, CentroCompetencia, 22 Jan. 2025, at https://centrocompetencia.com/brazil-ex-ante-regulation-of-ecosystems-the-clash-of-different-approaches-and-paths-forward/

[123] *It's getting personal*, footnote 11, p. 2

[124] Open Web Advocacy, *SLAP and FLOP: Apple's Lack of Full Site Isolation and iOS Browser Ban Puts Users at Risk*, 4 February 2025, at https://open-web-advocacy.org/blog/slap-and-flop--apples-lack-of-full-site-isolation-and-ios-browser-ban-puts-users-at-risk/

[125] *Ibid.*

competitors, reducing their incentives to develop it. But there are many other individual and overall security and privacy aspects of these designated services where the value of innovations can be captured by the gatekeeper.

In this way, interoperability can *increase* the incentives for companies to create trustworthy products and services.[126] And if Apple develops further security controls to reduce the amount of sensitive information (such as Wi-Fi universal identifiers and passwords) shared with all connected devices (including its own), as well as better enforcing iOS security and privacy restrictions (such as its Required Reason APIs and "Privacy Nutrition Labels"), that will increase security and privacy for its own users as well.

5.2.1. THE NECESSITY OF PUBLICLY-FUNDED RESEARCH AND DEVELOPMENT

Computing devices continue to face an extremely challenging threat environment, with continued research needed into how to meet these threats in the radically more connected societies which have evolved in Europe and elsewhere over the last decade – not least in developing mechanisms to evaluate the overall security and privacy protection levels of systems built from many (frequently untrusted) components from multiple sources.

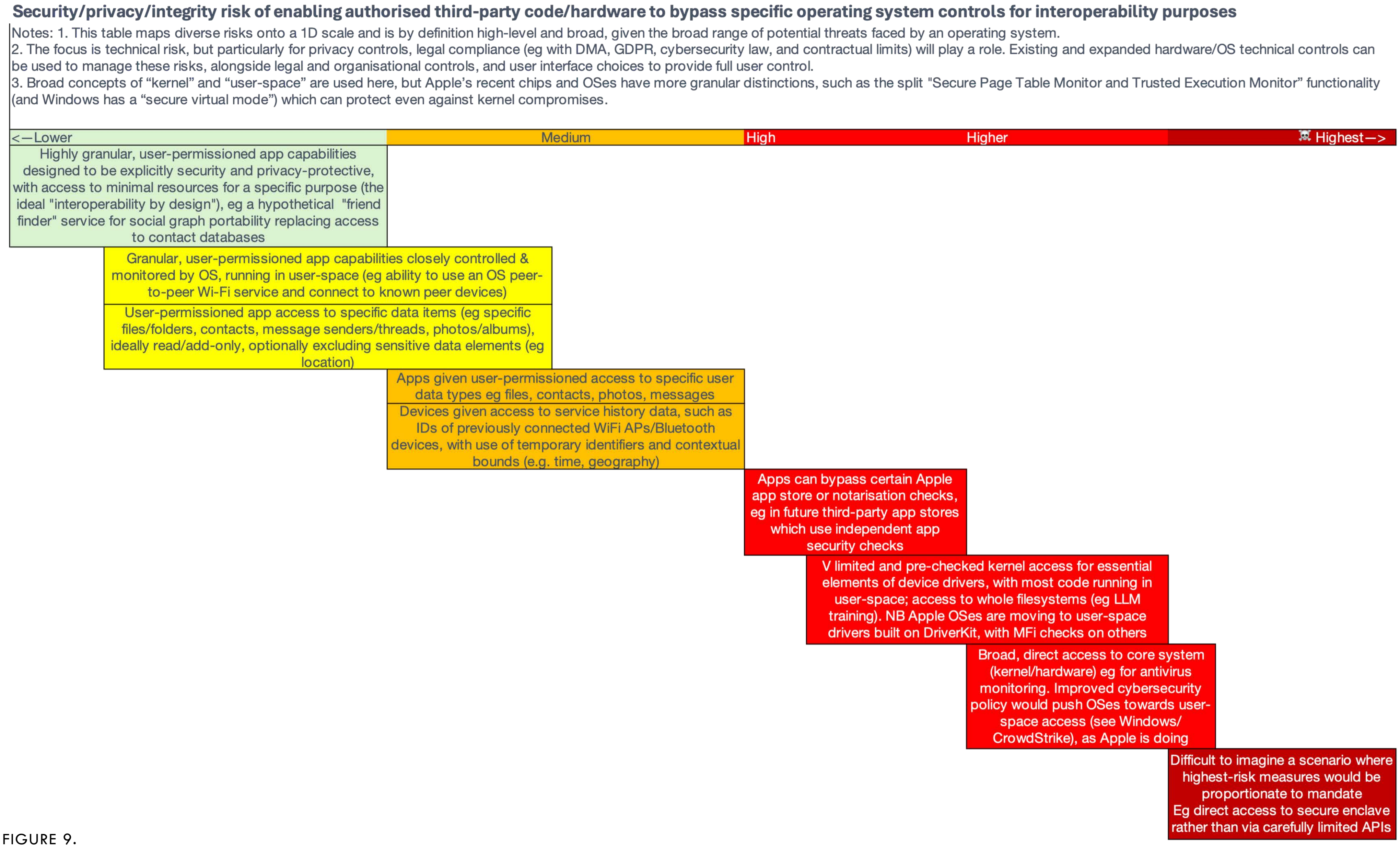
Recognising its societal benefits, the EC and EU member states can play an important role in meeting this challenge, by funding ongoing research and development on these topics – as it has done under its "increased cybersecurity"[127] Horizon Europe and many previous programmes.

[126] I. Brown, *Interoperability as a Tool for Competition Regulation*, OpenForum Academy, Nov. 2020, at https://openforumeurope.org/publications/ofa-research-paper-interoperability-as-a-tool-for-competition-regulation/

[127] European Research Executive Agency, at https://rea.ec.europa.eu/funding-and-grants/horizon-europe-cluster-3-civil-security-society/increased-cybersecurity_en

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

TABLE 2.



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

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

<—Lower | Medium | High | Higher | ☠ Highest—>

Highly granular, user-permissioned app capabilities designed to be explicitly security and privacy-protective, with access to minimal resources for a specific purpose (the ideal "interoperability by design"), eg a hypothetical "friend finder" service for social graph portability replacing access to contact databases

Granular, user-permissioned app capabilities closely controlled & monitored by OS, running in user-space (eg ability to use an OS peer-to-peer Wi-Fi service and connect to known peer devices)

User-permissioned app access to specific data items (eg specific files/folders, contacts, message senders/threads, photos/albums), ideally read/add-only, optionally excluding sensitive data elements (eg location)

Apps given user-permissioned access to specific user data types eg files, contacts, photos, messages

Devices given access to service history data, such as IDs of previously connected WiFi APs/Bluetooth devices, with use of temporary identifiers and contextual bounds (e.g. time, geography)

Apps can bypass certain Apple app store or notarisation checks, eg in future third-party app stores which use independent app security checks

V limited and pre-checked kernel access for essential elements of device drivers, with most code running in user-space; access to whole filesystems (eg LLM training). NB Apple OSes are moving to user-space drivers built on DriverKit, with MFi checks on others

Broad, direct access to core system (kernel/hardware) eg for antivirus monitoring. Improved cybersecurity policy would push OSes towards user-space access (see Windows/ CrowdStrike), as Apple is doing

Difficult to imagine a scenario where highest-risk measures would be proportionate to mandate
Eg direct access to secure enclave rather than via carefully limited APIs

FIGURE 9.

CTS-FGV Law School
Rio de Janeiro, RJ, Brazil, 2025
Cover image: Maximalfocus on Unsplash.

FGV DIREITO RIO
CENTRO DE TECNOLOGIA
E SOCIEDADE

FGV DIREITO RIO

CENTRO DE TECNOLOGIA
E SOCIEDADE