Assessing Apple’s strategy of Jan. 2024 to comply with the Digital Markets Act

***

The barriers against Device Neutrality

Free Software Foundation Europe

Feb, 2024

Table of Contents

Executive summary

This report lays down the assessment of Apple’s announcement of its compliance strategy plan with the Digital Markets Act (DMA) in January, 2024, the impact over “Device Neutrality” and Free Software in general. Since the compliance procedures are dynamic, the conclusions of this report are, therefore, provisional. The conclusions of this paper do not configure legal/economic/business advice.

Closer examination of Apple’s plans reveals some fragilities in relation to DMA compliance, and the introduction of severe risks for developers and users’ software freedom, tighter control over the Apps Store and increasing switching costs for users in relation to their personal data. This report concludes that, while the DMA aims to promote contestability and fairness, Apple's proposed changes may reinforce its monopolistic behaviours by restricting software freedom, strengthening the dependency of developers and users to its own services and products and increasing switching costs.

Besides underscoring the urgency to impose strict observance of DMA rules to the designated gatekeepers, this report also highlights the necessity to safeguard Device Neutrality in broader terms by promoting higher degrees of software freedom, weakening vendor and manufacturer lock ins and better policies for end-user control over data.

Glossary

"App store": An entity that provides services for mobile application ingestion, review, and distribution.

(3PAS): "3rd-party app store" an app store service run by a non-Apple organization.

(3PASA): "3rd-party app store app" the actual program, approved by Apple and available for side-loading via direct download (e.g, from a web page), that enables users to download and install apps provided by the 3PAS.

(AAS): Apple App Store: the app store service run by Apple Inc.

(AASA): Apple App Store app: The actual program, pre-installed on all iOS devices, that enables users to download and install Apple-approved apps.

(ASC): „App Store Connect“

DMA: Digital Markets Act

EC: European Commission

EU Charter: Charter of fundamental rights of the European Union

ECJ: European Court of Justice

FSFE: Free Software Foundation Europe

Side-loading: The act of installing a program on a device directly, either from a web page or other means, without going through an App store.

Introduction

The FSFE deeply appreciates the opportunity to present its opinion to the Headquarters for Digital Market Competition of Japan (HDMC) on Apple's new strategy to comply with DMA and its impact on Free Software (also known as Open Source Software).

The FSFE has a 20-years expertise working with competition law matters. Besides being involved with strategic litigation in Europe (Microsoft case), it has participated in the Digital Markets Act (DMA) legislative process, collaborating with members of the European Parliament. The FSFE has also worked with competition and telecommunications regulators all over Europe in the topics related to digital devices and Free Software. We are happy and honoured to collaborate with HDMC.

The dominant power of corporations like Apple over digital devices has sparked policy, regulatory, and legal reactions trying to impose accountability on such large enterprises controlling how end-users should use their equipment. The DMA addresses companies exercising control over whole platform ecosystems in the digital economy and are structurally extremely difficult to challenge or contest by existing or new market operators, irrespective of how innovative and efficient those market operators may be (Recital 3).

In September 2023, the European Commission (EC) has designated Apple as gatekeeper under Art. 3 DMA by determining the following services as gateway for business users to reach end users: (i) Apple's online intermediation service App Store; (ii) Apple's operating system iOS; and (iii) Apple's web browser Safari.

In regards to this decision, Apple endeavoured two approaches: the company appealed of the EC's decision in December, 2023 to the European Court of Justice (ECJ) (T-1080/23), and announced in January, 2024 changes to iOS, Safari and the App Store to comply with the DMA. The proposed changes will commence with the iOS 17.4 version. This report will focus on App Store and iOS.

Closer examination of Apple's plans reveals some fragilities in relation to DMA compliance, and the introduction of severe risks for developers and users' software freedom, tighter control over the Apps Store and increasing switching costs for users in relation to their personal data. This report concludes that, while the DMA aims to promote contestability and fairness, Apple's proposed changes may reinforce its monopolistic behaviours by restricting software freedom, strengthening the dependency of developers and users to its own services and products and increasing switching costs.

Besides underscoring the urgency to impose strict observance of DMA rules to the designated gatekeepers, this report also highlights the necessity to safeguard Device Neutrality in broader terms by promoting higher degrees of software freedom, weakening vendor and manufacturer lock ins and better policies for end-user control over data.

Apple's online intermediation service App Store

Apple exercises a tight-knitted centralized control over the app store infrastructure. Apple operates its App Store as a unified digital store front across various platforms, including:

- App Store on iPhones ("iOS App Store");
- App Store on iPads ("iPadOS App Store");

- App Store on Mac computers (“macOS App Store”);
- App Store on Apple TVs (“tvOS App Store”); and
- App Store on Apple Watches (“watchOS App Store”).

While Apple affirms that each of its five app stores constitutes a distinct CPS under the DMA, the FSFE is of the opinion (similarly to the EC) that while there are nuances in the application availability and functionality across these platforms, - the underlying structure and governance are consistent, representing a single, integrated ecosystem rather than distinct app stores for each platform:

(a) the App Store is used for the same purpose from both an end user and a business user perspective across all devices on which it is available, namely to intermediate the distribution of applications.

(b) Apple provides a common framework of agreements governing Apple’s legal relationship with app developers, such as the Apple Developer Program License Agreement and the Apple Developer Agreement. These agreements apply to all of Apple’s app developers, regardless of the device and operating system on which they distribute their apps.

(c) Apple’s documentation regarding policies, agreements and guidelines apply across devices, for instance:

    (a) the agreement on the use of application development tools, in particular the Xcode and SDKs Agreement. This agreement contains a reference to the distribution of apps developed for specific operating systems through the (single) App Store;

    (b) the privacy policy to app developers;

    (c) the advertising policies applicable on the App Store;

    (d) Marketing and Identity Guidelines, and others.

While the DMA is compelling Apple to allow alternative app stores, the company is trying to maintain a significant level of control over its ecosystem. The new changes make the new changes look undesirable to make developers and users stick to the status quo in several ways, reinforcing Apple’s gatekeeping position.

Apple’s new terms for iOS 17.4

A closer examination of the press release and Apple’s developers support page reveals that requirements the alternative app store developers will have to meet are undesirable and unreasonably extensive. The FSFE understands that several requirements directly go against the DMA, and will reinforce its gatekeeper position. In this section we focus on the recent changes introduced by Apple and its potential non-conformity with DMA.

Changes proposed by Apple for iOS 17.4 in relation to third-party app stores[1]

#	Apple iPhone App Store (Current System)	Alternative iPhone App Marketplaces (New)	Android 3rd-party apps stores [Comparison]
1	Developers register with Apple, T&Cs, $99/year	Developers register with Apple, T&Cs, $99/year	No Google developer registration requirement
2	Mandatory app review for functionality, security, policy, content	Mandatory app review for functionality & security	Google lets users select which review from the device itself
3	Apps ingested through App Store Connect and encrypted with DRM	Apps ingested through App Store Connect and encrypted with DRM	No DRM or encryption applied to apps
4	Apps distributed via Apple App Store only	Apps distributed via Apple App Store or a third-party app store which must be based in EU and provide annual €1M letter of credit	Apps distributed via Google Play Store, Samsung Store, Amazon Store, F-Droid, etc.
5	No side-loading	No side-loading, with the sole exception of Apple-approved 3rd party app store apps themselves; every other app must either be installed either through one of these 3rd party app store apps, or through the Apple App Store app	Side-loading permitted by direct download of .apk from any source
6	30% commission on all digital commerce	€0.50/install Core Technology Fee	No fee for downloads or commission on digital commerce

Discrimination via terms and conditions (#1 and #6)

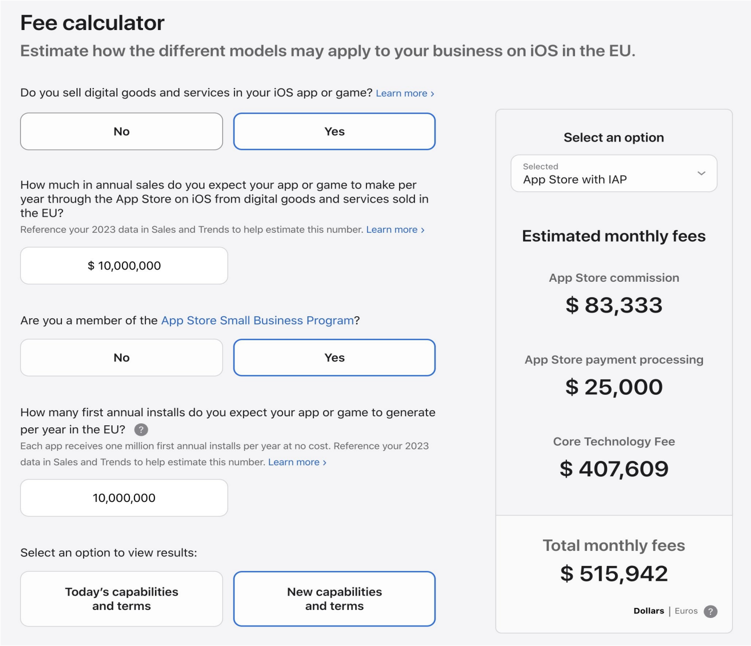
Although there was no significant change in the new terms, Apple Developer Program still represents a considerable barrier for third party developers wanting to distribute apps for Apple devices in two ways: the imposition of Apple tool kit for app development and the yearly fee represent unduly discrimination towards smaller FOSS developers that do not posses the capacity to scale to meet such requirements.

Until now, Apple charged 30% commission on all digital commerce within the companies ecosystem. Apple has introduced several smaller fees,[2] including the “core technology fee”, which will disproportionately affect those app developers that have limited revenues, but whose apps are widely downloaded. These commissions are not fair and reasonable and are not compliant with Article 6(12) and (13) and recital 52 DMA.

[1] Table retrieved from: Prud'hommeaux, Marc. *iPhone App Marketplaces Changes proposed by Apple for iOS 17.4*. Presentation slides on the App Fair Project. 12.02.2024.

[2] "App Store iOS apps will be subject to a reduced commission rate of either 17% on transactions for digital goods and services, or 10% (for the vast majority of developers and subscriptions after their first year), irrespective of the payment processing system chosen" "Payment processing fee—For an additional 3%, iOS applications available on the App Store may utilise the App Store's payment processing." Apple does not charge developers any additional fees when they link consumers to a website or utilise a Payment Service Provider within their application to process payments.

As a matter of fact, the new "core technology fee" is unreasonable arbitrary and exploitative. [Several estimates](#) using [Apple's fee calculator](#) show that if there is an app with 10 million sales then Apple takes a 6.2 million cut in the sales. This amounts to 515,942 per month compared to 250,000 per month and 3 million per annum under the status quo. The screenshot below demonstrates Apple's new fee policies that have a negative impact on the developers.



Fee calculator

Estimate how the different models may apply to your business on iOS in the EU.

Do you sell digital goods and services in your iOS app or game? Learn more ›

No | Yes

How much in annual sales do you expect your app or game to make per year through the App Store on iOS from digital goods and services sold in the EU?

Reference your 2023 data in Sales and Trends to help estimate this number. Learn more ›

$ 10,000,000

Are you a member of the App Store Small Business Program?

No | Yes

How many first annual installs do you expect your app or game to generate per year in the EU? ?

Each app receives one million first annual installs per year at no cost. Reference your 2023 data in Sales and Trends to help estimate this number. Learn more ›

10,000,000

Select an option to view results:

Today's capabilities and terms | New capabilities and terms

Select an option

Selected: App Store with IAP

Estimated monthly fees

App Store commission: $ 83,333

App Store payment processing: $ 25,000

Core Technology Fee: $ 407,609

Total monthly fees: $ 515,942

Retrieved from apple website [Fee calculator](#)

Gatekeeper control via app review (#2)

Apple exercises a tight control over app review. While Apple has conducted review for functionality, security, policy, content, in the new terms the company has reduced the parameters for functionality and security. App review can be considered a legitimised curation activity by app stores and marketplaces. However, some review parameters can cause self-preference and discrimination when the same attitude is not equally applied to the same type of app.

No Side-loading (#3 and #5)

As with the previous terms, Apple still does not allow side-loading. The sole exception is Apple-approved 3rd party app store apps themselves; every other app must either be installed either through one of these 3rd party app store apps, or through the Apple App Store app. Developers who do not actively choose to accept Apple's new business terms, which will take effect in March 2024 (they can agree to the terms at any time, as per Apple's policy), will be automatically and technically prevented from distributing apps in app stores that are not native to Apple. According to Art. 6(4) DMA, Apple is required to permit side-loading. However, Apple is interpreting this requirement very narrowly.

As comparison, side-loading is still available on personal computers, including iMacs. Apple argues that the introduction of side-loading in the EU under the DMA will lead to a less secure system compared to the current model in the rest of the world. Apple uses this as a justification to implement various controls that will make their obligations under Article 6(4) DMA less clear. Apps will need to undergo notarization via proprietary DRM encryption regardless of how they are distributed. Apple exercises gatekeeper control on how an app is submitted to the Apple App Store and further distributed to the public. Any app developed for the App Store should be ingested through App Store Connect (ASC) and encrypted with Apple's proprietary DRM. The, the app's binary is provided in a encrypted manner via the App Store to the public. This system has not changed in the new terms. Apple's approach leads to extreme forms of control and consolidates its entrenched position of gatekeeper over its devices.

By forcing proprietary encryption via DRM over the submitted code, it is not possible to further audit the app's source code, since a credible reproducible build of the app is no longer possible. This has serious implications towards security – as third party auditors cannot certify the authenticity of the source code -, and to software freedom, as users are not allowed to check the source code of free and open source software without jailbreaking Apple's DRM.

Narrow enablement of 3rd-party app stores (#4)

With the new terms, 3rd party app stores and repositories (3PAS) will be allowed by Apple. However, Apple implements this DMA-related obligation very narrowly, and continues to exercise unreasonable control, such as requiring a 1 million euro letter of credit per year. In comparison, in the Android ecosystem, apps can be distributed not only via Google Play Store but also another 3rd party app stores.

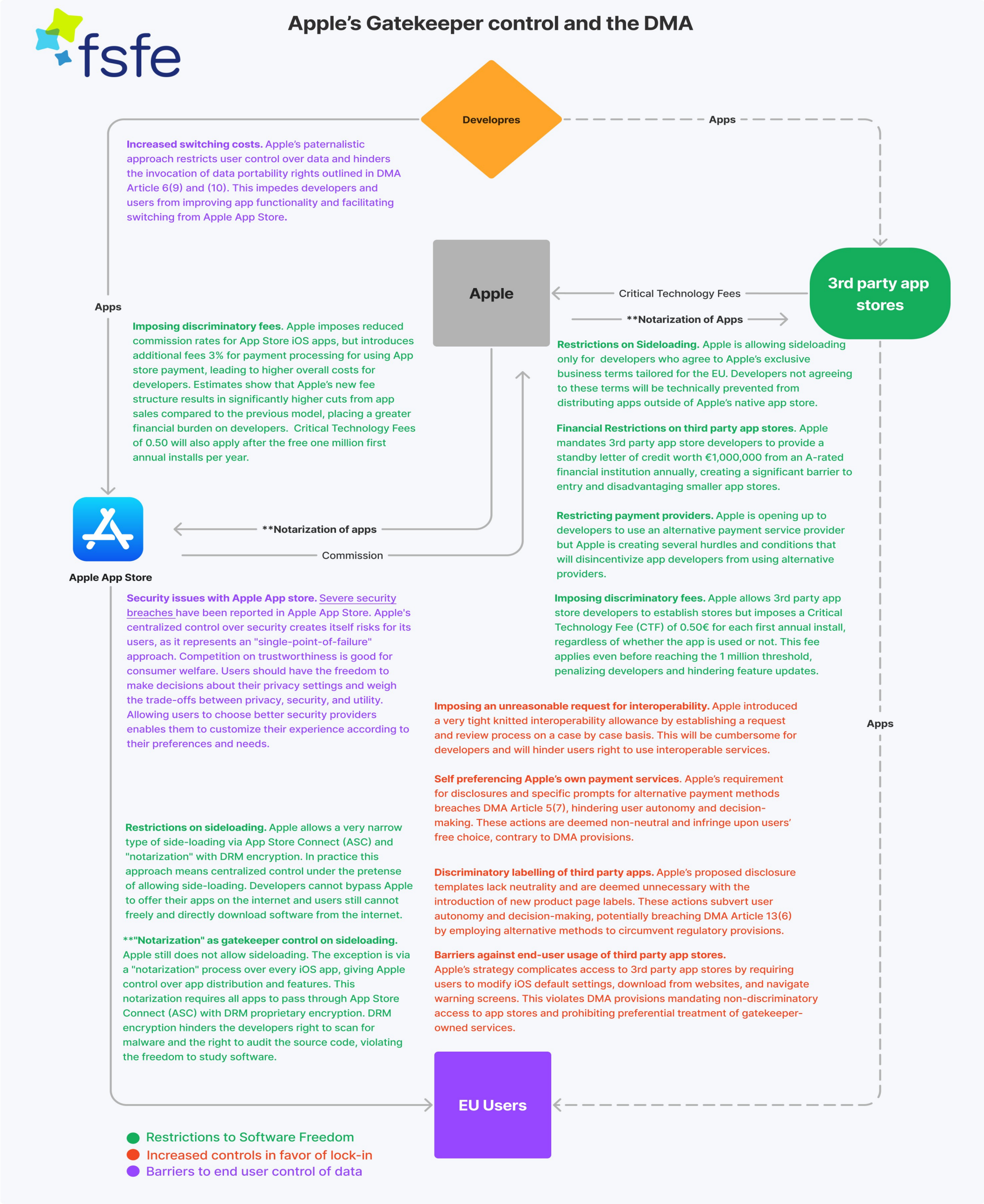
Apple will only grant 3rd party app store developers the ability to establish 3rd party app stores or repositories (3PAS), provided that they undertake substantial accountability and supervision regarding user experience while administering the said app stores. By retaining its control to grant app store developers permission to distribute specialized app stores for iOS apps, provided they satisfy particular requirements and commit to upholding ongoing criteria for safeguarding users and developers (referred to as Alternative App Marketplace Entitlement process). The developers of 3PAs will be accountable for the operation of their application stores, which appears to be reasonable. In addition, Apple will grant authorization to 3PAS developers who can provide a letter of credit from an A-rated financial institution in the amount of €1,000,000, with an annual renewal requirement. This immediately puts 3PAS developers at a huge disadvantage simply because it is a huge number and obtaining this letter of credit is not feasible for all the alternate app store developers.

Besides, according to these new business terms, the marketplace developers will be charged by Apple 0,50€ for each first annual install of their marketplace app above the 1MM threshold generated from the App store. Apple calls this as 'Critical Technology Fees' (CTF). Shockingly, the 1MM free first annual thresholds are not available for alternative app stores and so they will pay the CTF for every first annual install of the app, including installs that occur before the 1 million threshold is met. The definition of 'first annual install' is broad and vague. It includes the first installation of an app, as well as subsequent installations or updates from any iOS app distribution method within a 12-month time frame. So a developer would have to pay this fee even if a user downloaded the app, never used it and forgot to delete it.

The broad interpretation of first annual installations penalises developers who have a substantial number of existing users/limited number of users and undermines their motivation to release feature updates. Moreover, the stipulation that CTF is priced per install creates an obstacle for 3rd party app store (3PAS) developers to achieve the necessary scope to compete with Apple's proprietary App Store on merit.

Summary flowchart for app stores

The summary of the new terms and how they affect software freedom by increasing vendor lock-in and switching costs are given in the flowchart below.



Apple’s Gatekeeper control and the DMA

Increased switching costs. Apple’s paternalistic approach restricts user control over data and hinders the invocation of data portability rights outlined in DMA Article 6(9) and (10). This impedes developers and users from improving app functionality and facilitating switching from Apple App Store.

Imposing discriminatory fees. Apple imposes reduced commission rates for App Store iOS apps, but introduces additional fees 3% for payment processing for using App store payment, leading to higher overall costs for developers. Estimates show that Apple’s new fee structure results in significantly higher cuts from app sales compared to the previous model, placing a greater financial burden on developers. Critical Technology Fees of 0.50 will also apply after the free one million first annual installs per year.

Restrictions on Sideloading. Apple is allowing sideloading only for developers who agree to Apple’s exclusive business terms tailored for the EU. Developers not agreeing to these terms will be technically prevented from distributing apps outside of Apple’s native app store.

Financial Restrictions on third party app stores. Apple mandates 3rd party app store developers to provide a standby letter of credit worth €1,000,000 from an A-rated financial institution annually, creating a significant barrier to entry and disadvantaging smaller app stores.

Restricting payment providers. Apple is opening up to developers to use an alternative payment service provider but Apple is creating several hurdles and conditions that will disincentivize app developers from using alternative providers.

Imposing discriminatory fees. Apple allows 3rd party app store developers to establish stores but imposes a Critical Technology Fee (CTF) of 0.50€ for each first annual install, regardless of whether the app is used or not. This fee applies even before reaching the 1 million threshold, penalizing developers and hindering feature updates.

Security issues with Apple App store. Severe security breaches have been reported in Apple App Store. Apple's centralized control over security creates itself risks for its users, as it represents an "single-point-of-failure" approach. Competition on trustworthiness is good for consumer welfare. Users should have the freedom to make decisions about their privacy settings and weigh the trade-offs between privacy, security, and utility. Allowing users to choose better security providers enables them to customize their experience according to their preferences and needs.

Imposing an unreasonable request for interoperability. Apple introduced a very tight knitted interoperability allowance by establishing a request and review process on a case by case basis. This will be cumbersome for developers and will hinder users right to use interoperable services.

Self preferencing Apple’s own payment services. Apple’s requirement for disclosures and specific prompts for alternative payment methods breaches DMA Article 5(7), hindering user autonomy and decision-making. These actions are deemed non-neutral and infringe upon users’ free choice, contrary to DMA provisions.

Restrictions on sideloading. Apple allows a very narrow type of side-loading via App Store Connect (ASC) and "notarization" with DRM encryption. In practice this approach means centralized control under the pretense of allowing side-loading. Developers cannot bypass Apple to offer their apps on the internet and users still cannot freely and directly download software from the internet.

****"Notarization" as gatekeeper control on sideloading.** Apple still does not allow sideloading. The exception is via a "notarization" process over every iOS app, giving Apple control over app distribution and features. This notarization requires all apps to pass through App Store Connect (ASC) with DRM proprietary encryption. DRM encryption hinders the developers right to scan for malware and the right to audit the source code, violating the freedom to study software.

Discriminatory labelling of third party apps. Apple’s proposed disclosure templates lack neutrality and are deemed unnecessary with the introduction of new product page labels. These actions subvert user autonomy and decision-making, potentially breaching DMA Article 13(6) by employing alternative methods to circumvent regulatory provisions.

Barriers against end-user usage of third party app stores. Apple’s strategy complicates access to 3rd party app stores by requiring users to modify iOS default settings, download from websites, and navigate warning screens. This violates DMA provisions mandating non-discriminatory access to app stores and prohibiting preferential treatment of gatekeeper-owned services.

- ● Restrictions to Software Freedom
- ● Increased controls in favor of lock-in
- ● Barriers to end user control of data

iOS interoperability and security issues

The DMA is introducing new interoperability rules that will apply to Apple's operating systems. The company offers five distinct operating systems. Each of these operating systems constitutes a distinct core platform service under Art. 3(2) DMA.

i. iOS (for Apple's smartphone, iPhone);
ii. iPadOS (for Apple's tablet, iPad);
iii. macOS (for Apple's laptop and desktop computer, Mac);
iv. watchOS (for Apple's smartwatch, Apple Watch); and
v. tvOS (for Apple's media streaming device designed to integrate with consumerTV sets, Apple TV).

The interoperability rules referred here are laid down in Art.6 (7) DMA. The objective is to promote interoperability which is an already established concept under the European directive for electronic communications. Interoperability allows for freedom of choice for users/consumers and improves interconnectivity within the internal market and thereby upholds consumer protection as per Art.38 of the EU Charter. In order to achieve the above-mentioned set goals it is genuinely necessary to restrict the gatekeepers dominant positions in the relevant market and mandate for interoperable standards.

The rationale for supporting the interoperability mandate is that its implementation would not compromise existing user security standards and would not infringe upon the EU Charter's protections for privacy and personal data. The reasonable level of security while keeping the interoperability mandates is that it can lead to increased competition and innovation in the messaging service market. By allowing users on different platforms to communicate with each other, it breaks down the barriers that currently exist and promotes a more open and competitive environment. This can incentivize service providers to improve their security measures in order to attract and retain users. With more users having the ability to choose their preferred messaging service, providers will have to prioritize security to gain a competitive edge. Additionally, interoperability can also lead to collaboration between service providers in addressing security challenges and sharing best practices. By working together, they can develop more robust security protocols and ensure that user data is protected across different platforms. Overall, achieving a reasonable level of security while maintaining interoperability can create a more secure and user-friendly messaging ecosystem.[3]

Aggrieved with the decision that designates iOS as core platform service (CPS) Apple appealed the designation decision because it requires the company to comply with interoperability standards set out in Art 6 (7) DMA.

Besides, Apple has opted to establish a request form for enabling interoperability with iOS and iPhone features on a case-by-case basis. The FSFE considers this request form as

[3] Blessing, J. (2023). One Protocol to Rule Them All? On Securing Interoperable Messaging. In: Stajano, F., Matyáš, V., Christianson, B., Anderson, J. (eds) Security Protocols XXVIII. Security Protocols 2023. Lecture Notes in Computer Science, vol 14186.

unreasonable and only demonstrates Apple’s gatekeeping power. This approach is discriminatory and will create self-preference to Apple’s services or affiliates.

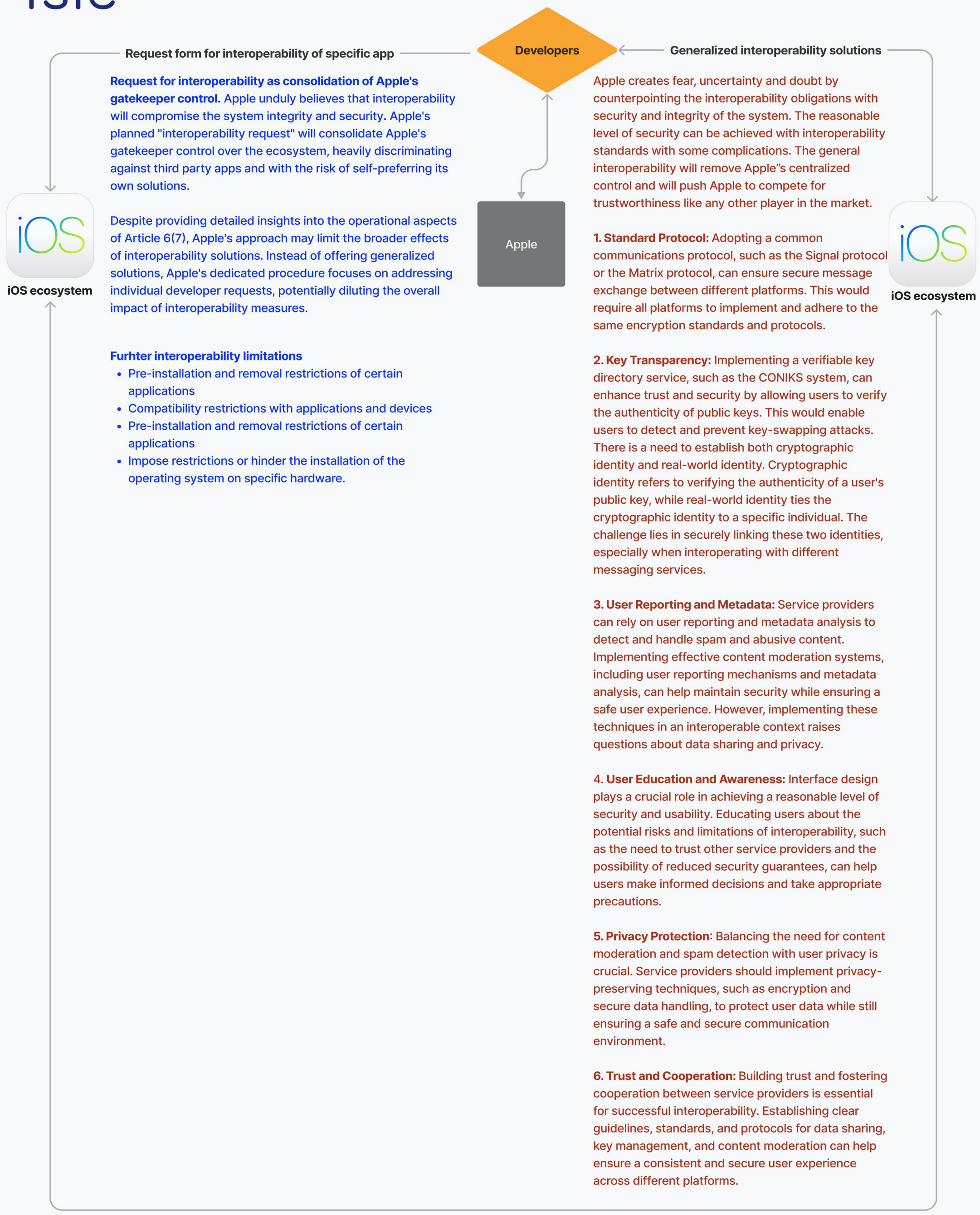
Apple unduly believes that interoperability will compromise the system integrity and security. Apple's planned "interoperability request form" will consolidate Apple's gatekeeper control over the ecosystem, heavily discriminating against third party apps and with the risk of self-preferring its own solutions.

Severe security breaches have been reported in Apple App Store and evidence against Apple App Store mishandling privacy of users have been raised in the US courts. Apple's centralised control over security and privacy creates itself risks for its users, as it represents an "single-point-of-failure" approach. Competition on trustworthiness is good for consumer welfare. Users should have the freedom to make decisions about their privacy settings and weigh the trade-offs between privacy, security, and utility. Allowing users to choose better security providers enables them to customize their experience according to their preferences and needs.

Summary flow chart for interoperability and security

A summary of barriers for interoperability and security imposed on iOS along with technical solutions for maintaining interoperability and security hand in hand can be found in the flowchart below.

Barriers on Interoperability and security


Developers
Apple
iOS ecosystem
iOS ecosystem
Request form for interoperability of specific app
Generalized interoperability solutions

Request for interoperability as consolidation of Apple's gatekeeper control. Apple unduly believes that interoperability will compromise the system integrity and security. Apple's planned "interoperability request" will consolidate Apple's gatekeeper control over the ecosystem, heavily discriminating against third party apps and with the risk of self-preferring its own solutions.

Despite providing detailed insights into the operational aspects of Article 6(7), Apple's approach may limit the broader effects of interoperability solutions. Instead of offering generalized solutions, Apple's dedicated procedure focuses on addressing individual developer requests, potentially diluting the overall impact of interoperability measures.

Furhter interoperability limitations

- Pre-installation and removal restrictions of certain applications
- Compatibility restrictions with applications and devices
- Pre-installation and removal restrictions of certain applications
- Impose restrictions or hinder the installation of the operating system on specific hardware.

Apple creates fear, uncertainty and doubt by counterpointing the interoperability obligations with security and integrity of the system. The reasonable level of security can be achieved with interoperability standards with some complications. The general interoperability will remove Apple"s centralized control and will push Apple to compete for trustworthiness like any other player in the market.

1. Standard Protocol: Adopting a common communications protocol, such as the Signal protocol or the Matrix protocol, can ensure secure message exchange between different platforms. This would require all platforms to implement and adhere to the same encryption standards and protocols.

2. Key Transparency: Implementing a verifiable key directory service, such as the CONIKS system, can enhance trust and security by allowing users to verify the authenticity of public keys. This would enable users to detect and prevent key-swapping attacks. There is a need to establish both cryptographic identity and real-world identity. Cryptographic identity refers to verifying the authenticity of a user's public key, while real-world identity ties the cryptographic identity to a specific individual. The challenge lies in securely linking these two identities, especially when interoperating with different messaging services.

3. User Reporting and Metadata: Service providers can rely on user reporting and metadata analysis to detect and handle spam and abusive content. Implementing effective content moderation systems, including user reporting mechanisms and metadata analysis, can help maintain security while ensuring a safe user experience. However, implementing these techniques in an interoperable context raises questions about data sharing and privacy.

4. **User Education and Awareness:** Interface design plays a crucial role in achieving a reasonable level of security and usability. Educating users about the potential risks and limitations of interoperability, such as the need to trust other service providers and the possibility of reduced security guarantees, can help users make informed decisions and take appropriate precautions.

5. Privacy Protection: Balancing the need for content moderation and spam detection with user privacy is crucial. Service providers should implement privacy-preserving techniques, such as encryption and secure data handling, to protect user data while still ensuring a safe and secure communication environment.

6. Trust and Cooperation: Building trust and fostering cooperation between service providers is essential for successful interoperability. Establishing clear guidelines, standards, and protocols for data sharing, key management, and content moderation can help ensure a consistent and secure user experience across different platforms.

FSFE’s demands: a claim for device neutrality

Gatekeepers with monopolistic behaviours impede software freedom, trap end-users in lock-ins and hinder personal control over data. Besides the negative effects on market competition, such behaviour negatively affects consumer welfare and digital sovereignty. At the heart of this issue lies the restriction on users' ability to freely install, run, and uninstall software on their devices, primarily motivated by commercial interests rather than security or privacy concerns. The FSFE runs the EU-wide initiative “Device Neutrality & Free Software” to raise awareness for policy topics regarding Free Software usage in devices, including the provisions of the DMA.

Apple’ reaction to the DMA turned the terms and conditions of Apple’s App Store even worse than before. The revised pricing structure should not negatively impact the competitive dynamics of the ecosystem for developers, specifically for business users. If developers experience a negative impact from Apple's refined cost structure and are consequently compelled to adhere to the existing business terms that already govern them, the DMA will fail to effectively equalise the competitive landscape in both the upstream and downstream aspects of app distribution.

Although the DMA represents a significant step forward in achieving fairness and contestability of digital markets, the FSFE is of the opinion that it is not enough. Higher degrees of openness and equality in digital markets can only be achieved by profound reforms on business models of large corporations such as Apple acting as gatekeepers when principles of device neutrality are incorporated by default in their business practices.

Higher degrees of software freedom

- Apple should enable business and end-users to install 3rd party app stores without financial and technological hurdles.
- Apple should enable completely and unfettered third-party software installation (side-loading) without the DRM-based encryption system for distribution.

Protecting users from lock-in and higher switching costs

- Apple should not be allowed to control app ingest and further distribution via DRM encryption (“notarization” in the new terms).
- Apple should not impose fees for app installs/updates.
- Apple should enable user control over app review processes.
- Apple should not be allowed to impose residency or credit requirements for establishing 3rd party app stores or marketplaces.
- Apple should not be allowed to impose “interoperability request forms”.
- Apple should compete on trustworthiness and let users choose their security and privacy providers.

Further information

Device Neutrality and Free Software

Contact information

- Dr. Lucas Lasota – FSFE Programme Manager

  lucas.lasota@fsfe.org