Recap on vertical interoperability under the DMA: Assessing Apple's compliance policy for Art. 6(7) from the perspective of FOSS[1]

Lucas Lasota, MA, PhD[2]
Jithendra Palepu, LLM[3]

Abstract: This article delves into the vertical interoperability obligations of the EU's Digital Markets Act. It provides a perspective that combines an analysis of the compliance approaches from gatekeepers in relation to Art. 6(7) DMA with a report over the experiences from free and open source software projects (FOSS) in requesting interoperability. The study concentrates on Apple as gatekeeper and portray diverse challenges involved in granting interoperability. The article concludes with lessons learned from regulatory activity over interconnection of terminal equipment (routers and modems) as examples of liberalization processes involving interoperability and end-user devices for internet connection.

Keywords: interoperability, DMA, Apple, compliance, competition, open source

1 This article does not necessarily reflect the views of any organisation the authors may represent.

2 Associate Researcher at Weizenbaum Institute (Berlin) and Legal Programme Manager at the Free Software Foundation Europe. Email: lucas.lasota@hu-berlin.de.

3 Independent researcher. Volunteer in the legal area at the Free Software Foundation Europe. Email: jithendra@fsfe.org.

Table of Contents

Introduction: entangling interoperability, DMA and FOSS

As societies grow in complexity, interoperability of assets and infrastructure becomes inevitable[4]. From urban engineering to transport, energy, healthcare and ICT industries, interoperability has been maximizing opportunities and facilitating human interaction[5]. In the EU, the liberalization of telecommunications has seen the usage of interoperability as a tool for expanding connectivity and opening up incumbents' infrastructure[6]. By addressing the competitive advantages enjoyed by former monopolies, interoperability enabled effective entry of new competitors[7]. The emergence of electronic communications[8] and the consequent digitalisation processes consolidated interoperability as a key element for promoting not only competition in digital markets but also openess and neutrality of the digital sector[9].

Historically, interoperability is marked by a striking contradiction: while market actors benefit from interoperability, they step back and react when their assets become important enough to be subject to interoperability obligations. Such behaviour can be tracked back to the emergence of industrial society but is still present in the digital age[10]. The interdependence of liberalisation and privatisation of ICT industries demonstrated this contrast starkly by revealing the market failures of the digital sector. The continuous waves of economic deregulation over the past 30 years in the US and EU have granted tech corporations broad access and control over crucial elements and components of digital ecosystems[11]. Such concentrated corporate power has been reflected in an unsustainable extraction of value from common digital assets and infrastructures, disrupting not only markets and welfare, but also the very notion of democracy[12]. Reactions to the deregulation-oriented mindset permeate a broad spectrum of agendas passing through grassroots movements, industrial policy and institutional reforms[13]. Interoperability became too important for being coordinated exclusively by market forces, being increasingly subject of policy and legislation.

In this context, open technologies acquire particular importance due to their strategic and competitive advantages[14]. Free and open source software (FOSS)[15], open protocols and open standards have been

4 See e.g. a historical perspective of interconnected complex systems. Palfrey, J., Gasser, U. (2012) *Interop: The promise and Perils of Higly Interconnected Systems*. Basic Books.

5 See Benkler, Y. (2006) *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. Yale University Press.

6 Savin, A. (2018) *EU Telecommunications Law*. Elgar, pp. 93-131; Cave, M., Genakos, C., Valletti, T. (2019) The European Framework for Regulating Telecommunications: A 25-year Appraisal. *Review of Industrial Organisation*, v. 55, pp. 47–62.

7 Manganelli, A., Nicita, A. (2020) *The Governance of Telecom Markets.* Palgrave Studies in Institutions, Economics and Law, pp. 1-35.

8 See Recital 148 of the European Electronic Communications Code. EU (2018) *Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) (Text with EEA relevance)*. ELI: http://data.europa.eu/eli/dir/2018/1972/oj.

9 See Recitals 1 and 4 of the Open Internet Regulation. EU (2015) *Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (Text with EEA relevance)*. ELI: http://data.europa.eu/eli/reg/2015/2120/oj

10 See the sociological analysis of power structures related to the Internet in Tarnoff, B. (2022) *Internet for the people: The fight for our digital future*. Verso Books, p. 8.

11 See e.g. the analysis conducted by Powers, M., Jablonski, M. (2015) *The Real Cyber War: The Political Economy of Internet Freedom.* University of Illinois Press.

12 Couldry, N., Mejias, U. (2019) *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism.* Stanford University Press.

13 Lasota, L. (2023) Regulating Corporate Behaviour in Digital Ecosystems: Increasing Fairness and Contestability of Digital Markets with Free Software. In Laporšek, S., et al (Orgs.) *MIC 2023: Toward Green, Inclusive, and Digital Growth*. University of Primorska Press. https://doi.org/10.26493/978-961-293-306-7. Accessed 30.10.24, p. 193.

14 Lasota, L. (2023), p. 194.

15 For a definition of Free and Open Source Software, see: Cyber Resilience Act, Art. 3 (40a): *'free and open-source software' means software the source code of which is openly shared and which is made available under a free and open-source license which provides for all rights to make it freely accessible, usable, modifiable and redistributable*. Council

key enabling factors for interoperability[16]. The permissive copyright and patent licensing terms (in comparison with proprietary software) permit the design, operational use and reuse of interoperable solutions (e.g. software components, APIs, standards, protocols), avoiding lock-in effects under democratic governance. Interoperability based on open technologies has been promoted in the EU as a foundational policy for Europe's digital infrastructure[17], digitalisation of the European public sector[18] and the future of internet technologies[19].

The ability of users to exercise the "four freedoms" of FOSS can come up against political, legal and economic factors which tend instead to put them into closed environments under the control of companies acting as gatekeepers. Such limitations have become more evident with mobile devices[20]. The complex environment of interconnected software, hardware and services has posed significant challenges for fair competition as mobile ecosystems are currently an oligopolistic market[21] where two players – Apple and Google – own the two leading mobile operating systems (iOS and Android), app stores (App Store and Google Play) and web browsers (Safari and Chrome). Notwithstanding that the products and services offered by Apple and Google have become to a great extent essential for the digital society, their mobile devices remain a fragile link to achieving an open and neutral internet[22].

Considering that the software industry in the EU is almost entirely composed of small and medium enterprises (SMEs), and the very large majority (94%) of them are micro enterprises with fewer than nine employees[23], interoperability has the potential to serve as a mechanism to rebalance the power relations in digital markets. The Digital Markets Act (DMA)[24], as an outcome of a paradigm shift in competition regulation[25], reflects an interventionist approach that applies interoperability as a key instrument to achieve fairness and contestability of digital markets. The DMA is a component of a broader industrial policy[26] aimed at the consolidation of the EU's internal market by promoting more

of the European Union (2023) *Interinstitutional File: 2022/0272(COD). Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. 17000/23*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=consil:ST_17000_2023_INIT. Accessed 30.10.24.

16 See e.g. DeNardis, L. (2011) *Opening Standards: The Global Politics of Interoperability*. MIT Press.

17 Keller, P., Krewer, J. (2024) *Mapping the Debates About Strengthening Europe's Digital Infrastructure*. Open Future. https://openfuture.eu/blog/mapping-the-debates-about-strengthening-europes-digital-infrastructure/. Accessed 30.10.2024.

18 EC (2017) *New European Interoperability Framework: Promoting seamless services and data flows for European public administration*. Luxembourg: Publications Office of the European Union. https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf. Accessed 30.10.2024, p. 14.

19 See e.g. the European Commission's Next Generation Internet funding program. Lasota, L., Ku Wei Bin, G. (2023) Managing Copyright and Licensing Information in Software Projects: Streamlining Specifications and Standards for the Next Generation Internet. In S. Laporšek, et al (Eds.) *MIC 2023: Toward Green, Inclusive, and Digital Growth*. University of Primorska Press. https://doi.org/10.26493/978-961-293-306-7.

20 See Krämer J., Feasey, R. (2021) *Device Neutrality: Openness, Non-Discrimination and Transparency on Mobile Devices for General Internet Access*. CERRE. https://cerre.eu/publications/mobile- devices-net-neutrality-internet-access/. Accessed on 30.10.2024.

21 Colangelo, G., Ribera, A. (2024) *Vertical Interoperability in Mobile Ecosystems: Will the DMA Deliver (What Competition Law Could Not)*? DEEP-IN Research Paper 2024. http://dx.doi.org/10.2139/ssrn.4826150. Accessed 05.11.24, p. 2.

22 ARCEP (2018) *Devices, the weak link in achieving an open internet. Report on their limitations and proposals for corrective measures*. https://www.arcep.fr/uploads/tx_gspublication/rapport-terminaux-fev2018-ENG.pdf. Accessed 30.10.2024.

23 EC (2022) *Commission Staff Working Document. Impact Assessment Report. Annexes to the Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. COM(2022) 454 final, SEC(2022) 321 final, SWD (2022) 283 final. Part 2/3*. https://ec.europa.eu/newsroom/dae/redirection/document/89546. Accessed 11.04.24, p. 29.

24 EU (2022) *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) (Text with EEA relevance)*. ELI: http://data.europa.eu/eli/reg/2022/1925/oj.

25 See e.g. the Chapter "The DMA as the Expression (and Endgame) of the New EU Competition Law" of Colomo (2023) *The New EU Competition Law*. Oxford: Hart Publishing, p. 124-152.

26 Tirole, J. (2024) Competition and industrial policy in the 21st century. *Oxford Open Economics*, v. 3.1. https://doi.org/10.1093/ooec/odad080. Accessed 30.10.24.

transparent, decentralized, inclusive and democratic institutional arrangements over the production, development and governance of key areas of the internet value chain[27]. Interoperability in the DMA performs two specific functions[28]: (i) to level the playing field between small and large market players; and (ii) to provide access to gatekeepers' functionalities, components and infrastructures upon which competitors rely and that they cannot easily replicate.

Against this background, FOSS and the DMA present a mutually beneficial relationship[29]. FOSS can serve the DMA's contestability goal by providing alternatives to the gatekeepers' restrictive proprietary closed environments. In turn, the DMA's attention to fairness in a variety of distributional issues (e.g. the allocation of rents, free-of-charge access to interoperability) has the potential to facilitate access to FOSS in devices. In 2019, the European Commission noted that, solely in that year, the investments in FOSS surpassed 1 billion euros, and small and micro enterprises could attribute over half their revenues to FOSS[30]. The plethora of FOSS solutions represents viable and fairer alternatives to proprietary-dominated environments that lead to monopolisation and restriction to consumer choice, especially in mobile ecosystems[31]. Smaller FOSS products and services do compete with gatekeepers, not by scale but in principles, i.e by offering curated app stores and repositories that can cater to a specific community's interests or user's interests[32]. Although the DMA has not set a specific regime for FOSS, contemporary EU legislation for cybersecurity[33], AI[34] and product liability[35] have contemplated peculiarities of this industry.

Adopting a culture of openness by default, FOSS fundamentally conflicts with gatekeepers' restrictive approaches to interoperability. Although restrictions to interoperability have been on the center of attention from scholars and regulators, a dedicated investigation from the perspective of FOSS was lacking. Therefore, the choice of Apple as a exemplar gatekeeper for this paper is not accidental, but important: achieving compliance with Apple may be a challenging endeavour, requiring tight regulatory oversight. By mantaining a tight control over sideloading, APIs and access to functionalities falling under Art. 6(4) and Art. 6(7), Apple has limited the potential of devices like the iPhone and iPads as general-purpose computers, affecting FOSS business-users and end-users.

The paper proceeds with examination of disputes, cases, contexts and regulatory solutions involving FOSS, interoperability and Apple as a gatekeeper. The exposition follows the contour of EU competition and telecommunications law to illustrate the expectations of the enforcement of the DMA. The paper concludes with the lessons learned from regulatory activity involving interconnection of personal routers and modems in the EU. Although the aspects of network interoperability in the Open

27 See e.g. EU (2023) *European Declaration on Digital Rights and Principles for the Digital Decade.* 2023/C 23/01. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001. Accessed 30.10.2024.

28 Bourreau, M. (2022) *DMA: Horizontal and Vertical Interoperability Obligations*. CERRE. https://cerre.eu/wp-content/uploads/2022/11/DMA_HorizontalandVerticalInteroperability.pdf. Accessed 30.10.2024, pp. 14-19.

29 Lasota (2023), p. 197.

30 EC (2022) *Commission Staff Working Document. Impact Assessment Report. Annexes to the Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. COM(2022) 454 final, SEC(2022) 321 final, SWD(2022) 283 final. Part 2/3*, p. 30.

31 FSFE (2024) *Feedback on Digital Markets Competition regime guidance: The significance of Free Software for fairer digital markets*. Berlin. https://download.fsfe.org/device-neutrality/fsfe-cma-dmcca-07-24.pdf. Accessed 30.10.24, p. 8.

32 See e.g. F-Droid for Android devices (https://f-droid.org/) and AppFair for iOS (https://appfair.org/en/).

33 See e.g. the discussion of the role of open source stewards in the Cyber Resilience Act in Stone, M. (2024) *Europe's Cyber Resilience Act: Redefining open source* https://securityintelligence.com/news/cyber-resilience-act-open-source/. Accessed 30.10.2024.

34 The AI Act introduces exceptions for models released under a free and open source license. See Recitals 102-104. EU (2024) *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance)*. ELI: http://data.europa.eu/eli/reg/2024/1689/oj.

35 The new Product Liability Directive includes exclusions for FOSS in Recitals 14 and 15. EP (2024) *European Parliament legislative resolution of 12 March 2024 on the proposal for a directive of the European Parliament and of the Council on liability for defective products (COM(2022)0495 – C9-0322/2022 – 2022/0302(COD))*. https://www.europarl.europa.eu/doceo/document/TA-9-2024-0132_EN.pdf. Accessed 30.10.2024.

Internet Regulation (EU) 2015/2120 related to freedom of terminal equipment are less complex, the regulatory solutions achieved in the liberalization processes in Germany, the Netherlands and Belgium serve as comparisons for opening up infrastructures and assets that once were subject to monopolistic control.

Vertical interoperability in the DMA

As a multidimensional concept, interoperability can be viewed from numerous perspectives and approached from various directions[36]. The taxonomy of interoperability[37] includes definitions encompassing different aspects i.a. technical (e.g. interface specifications and communication protocols allowing common functionalities across devices and systems), semantic (e.g. data with the same meaning and structure), organisational (e.g. aligned business processes) and legal (e.g. enabling organisations operating under different legal frameworks, policies and strategies to work together). Both telecommunications and digital markets have benefited from interoperability in their regulatory apparatus[38]. APIs[39], protocols, standards, formats, have been used as mechanisms to mandate shared access to an input or infrastructure, defining the terms and conditions of transactions among industry players and even in the design of products and business models[40].

Prior to the adoption of the DMA, a key expert report on digital markets ordered by the European Commission (EC)[41] distinguished between two types of interoperability: protocol interoperability, which allows technical interconnection between services or products, and full protocol interoperability, which enables substitute services, like messaging systems, to work together. Both forms rely on continuous or real-time access to user data, facilitated through application programming interfaces (APIs). In light of that, "*vertical*" and "*horizontal*" interoperability become useful to differentiate how features of gatekeepers' infrastructure and services are made accessible to third parties[42]. Horizontal interoperability refers to interactions between similar products or services (e.g. two different messaging apps), vertical interoperability denotes the interaction of asymmetrical products and services interacting together (e.g. a camera being accessed by a messaging app).

In the DMA, horizontal interoperability concerns messaging services ('number-independent interpersonal communications services' (NIICS)) in Art. 7. In turn, vertical interoperability, understood as access obligations to functionalities of operating systems or hardware capabilities of devices, are present in Art. 6(7), and the possibility to install third-party app stores and sideload apps in Art. 6(4). This study will focus on Art. 6(7). The main objective pursued with the interoperability mandate is to improve contestability (Recitals 54 and 64) and fairness (Recitals 50 and 54) of digital markets. Both horizontal and vertical interoperability level the playing field between small and large players and facilitate the entry of competitors by providing them access to gatekeepers' functionalities, components and infrastructures upon which competitors rely and that they cannot easily replicate[43].

36 Reza, R. et al (2014) Interoperability evaluation models: A systematic review. *Computers in Industry*, v. 65.1 pp. 1-23. https://doi.org/10.1016/j.compind.2013.09.001. Accessed 05.11.24.

37 See e.g. the Interoperability Framework proposed by the European Commission: EC (2017) *New European Interoperability Framework Promoting seamless services and data flows for European public administration*. Luxembourg: Publications Office of the European Union. https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf. Accessed 30.10.2024, pp. 21-30.

38 Brown, I. (2020) *The technical components of interoperability as a tool for competition regulation*. OpenForum Academy. https://www.openforumeurope.org/wp-content/uploads/2020/11/Ian_Brown_The_technical_components_of_interoperability_as_a_tool_for_competition_regulation.pdf. Accessed 30.10.2024.

39 An application programming interface (API) is a connection between computers or between computer programs. It is a type of software interface, offering a service to other pieces of software. More at: https://en.wikipedia.org/wiki/API.

40 Colomo, P. (2023) *The New EU Competition Law*. Oxford: Hart Publishing, p. 14.

41 Crémer, J., Montjoye, Y., Schweitzer, H. (2019) *Competition policy for the digital era*. European Commission, https://op.europa.eu/publication-detail/-/publication/21dc175c-7b76-11e9-9f05-01aa75ed71a1. Accessed 30.10.24.

42 Bourreau, M., Krämer, J., Buiten, M. (2022) *Interoperability in Digital Markets*. CERRE. https://cerre.eu/publications/interoperability-in-digital-markets/ Accessed 10.10.2024, pp. 19-36.

43 Bourreau, M. (2022) *DMA: Horizontal and Vertical Interoperability Obligations*. CERRE. https://cerre.eu/wp-content/uploads/2022/11/DMA_HorizontalandVerticalInteroperability.pdf. Accessed 30.10.2024, pp.

Vertical interoperability related to assets gatekeepers had chosen to keep for themselves. Due to its stringent effects, it is faced with resistance[44]. Degradation of interoperability involves not only technical apparatus but also contractual and commercial practices. Related practices have been traditionally evaluated in competition law under theories of discrimination, unfair terms and conditions, tying and bundling[45]. The broad vertical interoperability mandate in DMA contrasts with telecommunications, where interconnection requests concern only a few network elements[46]. By setting a higher interoperability standard, the DMA reacts to the limits of traditional competition law enforcement, where the profound market failures related to big tech's power demanded a paradigm shift in competition policy[47]. This change is particularly relevant since vertical interoperability – in order to be considered effective – should be guaranteed in a sustainable way and not as a one-off target[48]. Interoperability involves provisions aimed at opening gatekeepers' layers to rivals. Access duties amount to obligations to deal involving technologies the gatekeepers would rather keep to themselves. Remedies involving interoperability require intervention not only in how products and services are commercialized, but also in how they are originally designed. Interoperability obligations of Art. 6(7) represent a step further in traditional competition law by tackling issues of how products are sold and those addressing the way they are made, including product design and business-model related issues[49]. Similar to complex structural interventions in telecommunications, effective compliance with the interoperability mandate of Art. 6(7) requires substantial investments from gatekeepers and significant monitoring efforts from the Commission over time.

Apple as a gatekeeper under Art. 6(7) DMA

Apple's designation as a gatekeeper under the DMA[50] has the potential to transform Apple's digital ecosystem[51]. Apple's approach, often referred to as a "sandbox model", focuses on centralized control devices, which can be at odds with broad interoperability requirements. From a techinical-philosophical perspective, Apple's approach fundamentally difers from FOSS. FOSS development models prioritize open and persistent sharing of knowledge[52]. Businesses and communities access the wealth of knowledge via permissive (in comparison with proprietary) license terms that privately regulate the open, transparent interactions among members sharing information, resources and artefacts with very low entry barriers[53]. On the other side of the spectrum, Apple has focused on distinctive, technically and legally closed systems prioritizing internal compatibility among Apple devices against cross-platform interoperability[54]. Since Art. 6(7) provides free-of-charge and effective interoperability for third-party access seekers, the clash of philosophies become apparent. Alternative

14-19.

44 Bourreau, M. (2022), p. 12.

45 Colangelo, G., Ribera, A. (2024) *Vertical Interoperability in Mobile Ecosystems: Will the DMA Deliver (What Competition Law Could Not)*?, p. 6.

46 Bourreau, M. (2022), p. 16.

47 Colomo, P. (2023), pp. 124-152.

48 EC (2017) *New European Interoperability Framework Promoting seamless services and data flows for European public administration*, p. 23.

49 Colomo (2023), p. 242.

50 On September 2023, the Commission designated Apple's AppStore, iOS and Safari browser as Core Platforms Services. In May 2024, a further designation decision was issued for iPadOS. See EC (2023) *Commission Decision of 05.09.2023 designating Apple as a gatekeeper persuant Article 3 of Regulation (EU) 2022/1925 of the European Parliament and the Council on contestable and fair markets in the digital sector. DMA.100013 Apple – Online Intermediation Service – app stores, DMA.100025 Apple- operating systems and DMA.100027 Apple – web browsers*. https://ec.europa.eu/competition/digital_markets_act/cases/202344/DMA_100025_228.pdf; also EC (2024) *Commission Implementing Decision of 29.4.2024 closing the market investigation opened by Decision C(2023)6076, pursuant to Article 17 of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector and amending Commission Decision C(2023)6100 of 5 September 2023 designating Apple as a gatekeeper pursuant to Article 3 of that Regulation Case DMA.100047 Apple – iPadOS*. https://ec.europa.eu/competition/digital_markets_act/cases/202427/DMA_100047_5491.pdf. Accessed 30.10.24.

51 See the analysis of Colangelo, G., Ribera, A. (2024), pp. 14-18.

52 Serpico, D., Santini, E., Suksi, J. (2024) *3Os and IP Awareness raising for collaborative ecosystems - Innovation ecosystem report*. The Zooom Initiative. https://doi.org/10.5281/zenodo.10948750. p. 23

53 Serpico, D., Santini, E., Suksi, J. (2024), p. 24.

service providers and hardware manufacturers may access software and hardware features controlled by iOS via API features. Apple adopted a two-fold strategy facing the DMA. First, the company has questioned the constitutionality of DMA's interoperability mandate of Art. 6(7) in the appellate process at CJEU (T-1080/23)[55]. In this process, the company also questions the validity of the decision encompassing its App Store. In parallel, in its compliance report of February 2024, Apple introduced a "request for interoperability" submitting third parties to the company's scrutiny for granting access to software and hardware functionalities established by the law[56]. In September 2024, the Commission on its own initiative opened two specification proceedings on Apple's technical implementation of Art. 6(7), one for iOS connectivity features and functionalities and another for the procedural aspects of the request for interoperability[57]. This study will not focus on Apple's litigation actions but will elaborate more on the company's compliance approach in relation to vertical interoperability.

Art. 6(7) enables third-party developers to have the same ability as Apple to access functionalities and APIs of the operating system used by Apple. However, the DMA also includes a safety clause to avoid interoperability compromising "integrity of the operating system". Apple has relied on this to establish two main control barriers to interoperability access. The first relates to "notarization" for iOS and iPadOS. The second relates to the process by which interoperability is granted to access seekers. In the following sections, restrictive gatekeeping practices will be contextualized from the perspective of DMA.

Apple's "notarization" and vertical interoperability

The main venue for controlling "integrity" aspects of Apple's operating systems is the "notarization" process, also denominated "app review"[58]. This procedure combines automated checks and human review of platform policies for security, privacy, funtionality and policy. When applied to sideloading and enabling alternative app stores, notarization means also a subsequent re-signed and encrypted binary with proprietary DRM[59], which iOS requires in order for software to be installed[60]. Although app review can be considered a legitimised curation activity by app stores and marketplaces, some review parameters can cause self-preference and discrimination when the same attitude is not equally applied to access seekers[61]. 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 must be ingested through App Store Connect (ASC) and encrypted with Apple's proprietary DRM[62]. The app's binary is provided in an encrypted manner via the App Store to the public. This system behaves identically regardless of whether the app is distributed through Apple's App Store or a third-party app store.

54 See e.g. Sinofsky, S. (2024) *Building Under Regulation, An essay on the EU Digital Markets Act and Apple's "Update on apps distributed in the European Union" (and some personal history).* Hardcore Software. https://hardcoresoftware.learningbyshipping.com/p/215-building-under-regulation. Accessed 30.10.24.

55 Case T-1080/23: Action brought on 16 November 2023 — *Apple v Commission* [2023]. ELI: http://data.europa.eu/eli/C/2024/563/oj. Accessed 30.10.24.

56 Apple (2024) *Requesting interoperability with iOS and iPadOS in the European Union*. https://developer.apple.com/support/ios-interoperability/. Accessed 05.11.24. The request form remained unchanged in Apple's compliance report of 01.11.24.

57 See EC (2024) *Case DMA.100203 – Apple – Operating systems – iOS – Article 6(7) – SP – Features for Connected Physical Devices*. https://ec.europa.eu/competition/digital_markets_act/cases/202440/DMA_100203_76.pdf; and EC (2024) *Case DMA.100204 SP – Apple - Article 6(7) – Process*. https://ec.europa.eu/competition/digital_markets_act/cases/202440/DMA_100204_35.pdf. Accessed 05.11.24.

58 Apple (2024) *Apple's Non-Confidential Summary of DMA Compliance Report (01.11.24)*. https://www.apple.com/legal/dma/NCS-October-2024.pdf. Accessed 05.11.2024, p. 4.

59 Digital Rights (or Resctrictions) Management (DRM) relates to technical access control technologies. DRM can restrict the use of proprietary hardware and copyrighted works. Historically, the FOSS movement has taken a critical approach to DRM. More at: https://www.defectivebydesign.org/faq. Accessed 05.11.24.

60 FSFE (2024) *Assessing Apple's compliance with the Digital Markets Act: The barriers against Device Neutrality*. https://download.fsfe.org/device-neutrality/202404-FSFE-apple-report-EC.pdf. Accessed 01.10.24, p. 4.

61 FSFE (2024) *Assessing Apple's compliance with the Digital Markets Act: The barriers against Device Neutrality*, p. 10.

62 See App Store Connect instructions webpage: https://developer.apple.com/help/app-store-connect/. Accessed 05.11.24.

The impact of Apple's notarization on FOSS is manyfold. The most evident issue relates to transparent access to source code. After proprietary encryption via DRM of the submitted code, it is not possible to further audit the app's source code, since a credible reproducible build[63] of the app is no longer possible. This has implications for FOSS security – third party auditors cannot certify the authenticity of the source code. Further examples are provided in the next sections.

UTM emulator vs iOS notarization

Notarization can be wielded to either allow or deny interoperability, depending on Apple's strategic interests. A recent example, the blocking of the FOSS UTM PC emulator[64] via notarization, serves as an example[65]. UTM allows users to run virtual machines on Apple's devices, was barred from distribution outside of Apple's App Store due to notarization requirements. Although Apple relied on its guidelines which also allow game emulators, mini games, chatbots etc on App Store, the company stated "*PC is not a console*"[66]. This statement apparently does not consider the entire PC gaming industry which has been thriving for decades. This way Apple is blocking FOSS solutions that allow iPhone users to run other operating systems on their devices. This action by Apple demonstrates an instance where a claim of protecting the integrity of the operating system can limit the viability of third-party app stores, which Art. 6(4) and Art. 6(7) aim to protect. While Apple eventually allowed UTM to be distributed through its App Store[67], the incident raises a critical issue: if Apple - or any gatekeeper - can block what is available on independent third-party app stores, then DMA's interoperability mandate is at risk of violation. Such a situation underlines the importance of Arts. 6(4) and 6(7) working in tandem to prevent gatekeepers from arbitrarily deciding when and how interoperability is allowed.

Diverse notarization practices for Mac devices

Apple has diverse notarization procedures among its operating systems. Vertical interoperability is handled differently in Mac devices in comparison with iPhones and iPads[68]. Apple does not impose stringent notarization rules on Mac desktops and laptops[69]. In MacOS, developers and end-users enjoy unfettered third-party software installation (sideloading) without the DRM-based encryption system for distribution. Another example is Apple's own iOS *enterprise distribution program*[70], which allows organizations to create, sign, and distribute apps directly to users without intervention by Apple. Through this program, Apple effectively permits sideloading on iOS devices, but restricts it to large companies. Alledgly Apple already has the infrastructure and security protocols in place to allow third-party app distribution outside the App Store. Apple also allows sideloading of *Apple Music* (in the form of the *applemusic.apk* file)[71] on Android devices[72] but does not permit similar direct sideloading of, for instance, the S*potify.ipa* file on iOS.

---

63 Reproducible builds, also known as deterministic compilation, is a process of compiling software which ensures the resulting binary code can be reproduced. Source code compiled using deterministic compilation will always output the same binary. More at: https://en.wikipedia.org/wiki/Reproducible_builds. Accessed 05.11.24.

64 The UTM PC emulator allows business-users and end-users to run alternative operating systems in Apple devices. See UTM's source code repository at: https://github.com/utmapp/UTM. Accessed 30.10.24.

65 Peters, J. (2024) *Apple says no to PC emulators on iOS.* The Verge. https://www.theverge.com/2024/6/24/24185066/apple-pc-dos-emulators-ios-rejection. Accessed 30.10.24.

66 Rudra, S. (2024) *Apple Decides to Block Open-Source Emulator App for iOS*. It's FOSS News. https://news.itsfoss.com/apple-blocks-utm-se/. Accessed 30.10.24.

67 Davis, W. (2024), *After initially rejecting it, Apple has approved the first PC emulator for iOS.* The Verge. https://www.theverge.com/2024/7/13/24198015/apple-utm-se-pc-os-emulator-for-ios. Accessed 30.10.24.

68 Mac, short for Macintosh (its official name until 1999), is a family of personal computers designed and marketed by Apple. More at: https://en.wikipedia.org/wiki/Mac_(computer). Accessed 05.11.24.

69 Apple states "*Notarization of macOS software is not App Review*". See the notarization instructions for MacOS at: https://developer.apple.com/documentation/security/notarizing-macos-software-before-distribution. Accessed 05.11.24.

70 See the instructions webpage for the *Apple Developer Enterprise Program*, available at; https://developer.apple.com/programs/enterprise/. Accessed 30.11.24.

71 .APK is a file format used by the Android operating system for the distribution and installation of mobile apps and middleware. Windows PC software uses .EXE files for installation, and iOS uses .IPA files.. More at: https://en.wikipedia.org/wiki/Apk_(file_format). Accessed 05.11.24.

"Security paternalism" vs general-purpose computers

As noted by Merchant, Apple exercises a form of "security paternalism" over devices[73]. Such control, manifested already in 2000's policies[74] against jailbreaking of iPhones[75], artificially limitis the capabilities of iPhones as general purpose-computers. A general-purpose computer is defined as a machine designed to perform a wide range of computational tasks, rather than being restricted to a single, specialized function[76]. This close oversight and control over devices highlights the tension between user and manufacturer expectations of device ownership. Some voices claim that freedom of choice may not fully align with the complexity of modern mobile ecosystems, where the traditional general-purpose computer model would be viewed as outdated[77]. Others highlight the dangers of *toxic innovation* leading to monopolistic control over critical digital infrastructure the DMA aims to fix[78]. In *LG Electronics*, the CJEU held that smartphones, mobile phones, and wearable smart devices are similar to computers, thereby broadening the interpretation of what constitutes a "*computer*"[79]. This judgment supports the idea that these devices fall under the broader category of computing devices, which reinforce the arguments for requiring them to be interoperable with other systems and software. In the US, that the U.S. Copyright Office's Register also introduced an exemption in 2015 for jailbreaking underscoresd the principle of interoperability by permitting circumvention of access controls when it allowsed legally obtained applications to function on a device[80]. This exemption supports the notion that users should control their devices for compatible, non-infringing uses - ranging from accessibility modifications to third-party software enhancements. These cases outline the need to take a technologically neutral approach to devices in advancing interoperability and competition in digital ecosystems. By restricting devices that technically meet the criteria for general-purpose computing, Apple narrows their functionality and monopolizes app distribution, positioning itself contrary to the evolving standards for digital fairness and openness that Art. 6(7) seeks to promote. Recital 14 of the DMA reinforces the technological neutrality approach of the law. Computing devices - whether smartphones or traditional computers – are under the same regulatory framework, focusing on their functionalities, control, and interoperability rather than their specific form factors. By tightly controlling iOS and limiting interoperability, Apple undermines the versatile and open nature that a technology-neutral regulatory approach would otherwise seek to foster in general-purpose devices[81].

Interoperability grants under Art. 6(7)

The vertical interoperability provision of Art. 6(7) is broad, meaning gatekeepers should provide access to essential functionalities and assets controlled via the operating system that they use or make

72 See Apple's documentation for Android: "*Looking for Apple Music for your Android phone?"*, available at: https://www.apple.com/lae/apple-music/android-download/. Accessed 30.10.24

73 Merchant, B. (2017) *The One Device: The secret history of the iPhone*. Random House, p. 244.

74 Lohmann, F. (2009) *Apple says iPhone jailbreaking is illegal.* Electronic Frontier Foundation (EFF) https://www.eff.org/deeplinks/2009/02/apple-says-jailbreaking-illegal. Accessed 30.10.24.

75 Sometimes ompared to rooting an Android device, jailbreaking bypasses several types of Apple prohibitions for the end-user. Jailbreaking permits root access within the operating system and provides the right to install software unavailable through the App Store. More at: https://en.wikipedia.org/wiki/IOS_jailbreaking. Accessed 05.11.2024.

76 Freeman, J. (2012) *Comments on Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, DMCA.* U.S. Copyright office https://www.copyright.gov/1201/2012/comments/Jay_Freeman.pdf. Accessed 30.10.24.

77 See e.g. Sinofsky, S. (2024) *Building Under Regulation, An essay on the EU Digital Markets Act and Apple's "Update on apps distributed in the European Union" (and some personal history).*

78 Brown, I. (2024) *The randomness of US technologist views of the EU Digital Markets Act.* Data Protection and Digital Competition Blog, https://www.ianbrown.tech/2024/01/29/1592/. Accessed 30.10.24.

79 Case T-21/20, *LG Electronics Inc v European Union Intellectual Property Office (EUIPO)*, (2020) ECLI:EU:T:2020:550, §§ 51 and 53.

80 US Copyright Office (2015) *Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies. A Rule by the Copyright Office, Library of Congress on 10/28/2015.* https://www.federalregister.gov/d/2015-27212. Accessed 30.10.24.

81 Almada, M. (2024) *Two Dogmas of Technology-Neutral Regulation.* https://dx.doi.org/10.2139/ssrn.4953377. Accessed 30.10.24.

available for themselves. Apple, despite supporting numerous software development kits (SDKs)[82] and APIs for developer access, has introduced a process where developers must request enhanced interoperability on a case-by-case basis, retaining control over which requests are processed, approved or dismissed[83]. Recently, the Commission has manifested concerns about the procedural aspects of this interoperability request, especially due to lack of timely, transparent, and equitable solutions for third-party developers[84]. Indeed, although having a clear form for developers about topics regarding interoperability may simplify some aspects, the opaque decision-making may be at odds with the DMA. The interoperability grant referred to in Art. 6(7) is different from that in Art. 7(1) as the former does not require any form of approval or request for interoperability to be granted. Art. 6(7) is clear in saying that gatekeepers "*shall allow providers of services and providers of hardware, free of charge, effective interoperability*". Interoperability should be granted effectively, when access seekers meet the specifications of the APIs or any other channel involved in the interconnection. Only in narrow cases regarding integrity of the system should interoperability be reasonably and proportionately limited Other gatekeepers like Alphabet (Google) and Microsoft have also prepared compliance approaches to meet the requirements of Art. 6(7). The table below provides a bird's eye view for each of these.

82 A software development kit (SDK) is a collection of tools in one installable package. It facilitates the creation of applications by providing the necessary development elements specific to a hardware platform and operating system combination. More at: https://en.wikipedia.org/wiki/Software_development_kit. Accessed 30.10.24.

83 See Apple's *Requesting interoperability with iOS and iPadOS in the European Union*, available at: https://developer.apple.com/support/ios-interoperability/. Accessed 05.11.24.

84 EC (2024) *Case DMA.100204 SP – Apple - Article 6(7) – Process*, §§ 20-23.

Comparative table for Apple's, Alphabet's and Microsoft's approaches to Art. 6(7) DMA

	Apple[85]	Alphabet[86]	Microsoft[87]
Compliance approach	Interoperability grant via online request for Art. 6(7)[88]	Automatic interoperability grant for FOSS elements Online request for additional features under Art. 6(7)[89]	Automatic interoperability grant[90] Online request for Art. 6(7), 6(9), and 6(10)[91]
Description	Aside from the APIs made publicly available for developers, further interoperability requests from the EU should be done via the proposed online form.	FOSS elements of Google Android OS (AOSP) inherently support third-party interoperability. Google affirms Android permits third-party app and hardware developers to access and interoperate with the OS in the same way as Google's first-party apps and hardware. Additionally, Google has created a form for EU developers to request interoperability enhancements.	Microsoft applications use the same publicly documented APIs to call into Windows as are available to third-party applications. Microsoft attests the company and third-party applications can access the hardware and software features controlled by Windows. Microsoft provides an additional online form for DMA requests related to data and interoperability under the Art. 6(7), 6(9), and 6(10).
Procedure	Access to the request form requires an Apple account. Developers should reside in the EU. Developers' "Apple Developer Program membership" must be in good standing. Developers must have entered into the current terms of the Apple Developer Program License Agreement. Reviews consist of an initial assessment, a tentative plan and the development of the interoperability solution. Reviews are not public. The tentative plan will prioritize integrity of the operating system. The development of the solution should be highly specific to each request. Relevant technical documentation shall be provided. Updates should be given every 90 days.	The interoperability request form is located at AOSP Tracker. Access requires a Google account. The request is available for EU developers. Requests are public (visibility in the AOSP Tracker, meaning that other logged users are able see and interact with the request), or private at request of the developers. Developers are required to provide information on the functionality that a Google first-party app or service has access to and that a third-party app or service does not have access to. Developers are required to suggest a possible solution (access to specific API or calling third-party APIs) Reviews should take up to 6 weeks (42 days).	The interoperability request form is public. Developers can submit without an Microsoft account. Microsoft provides a common request form for Art. 6(7), 6(9) and 6(10), access seekers should choose under which regime their request should be processed. No information is given whether the requests are publicly available for third-parties. The response time and resolution plan may vary depending on the nature and complexity of the request. A case number is given up to three working days. No deadline for the review is given.
Decision making	Apple evaluates each request case-by-case and retains discretion over approvals and rejections. Integrity of iOS and iPadOS is one of the most important factors. Development decisons are highly specific to the request and depend on feasibility under the DMA. No regress procedure or external audit is provided. Developers can communicate back in the email thread.	No information on the decison making is provided.	Microsoft still exercises discretion to protect the integrity of the OS. The company may block malicious applications from accessing the APIs that its products and services rely upon.
Guidelines for integrity of the OS	Documentation on "app security review" publicly provided[92].	Documentation for "malware and unwanted software" publicly provided[93].	Documentation on "malware and potentially unwanted applications identification" publicly provided[94].

85 Apple (2024) *Apple's Non-Confidential Summary of DMA Compliance Report*. https://www.apple.com/legal/dma/NCS-October-2024.pdf. Accessed 05.11.24, pp. 7-8.

86 Alphabet (2024) *EU Digital Markets Act (EU DMA) Compliance Report Non-Condential Summary*. https://storage.googleapis.com/transparencyreport/report-downloads/pdf-report-bb_2023-9-6_2024-3-6_en_v1.pdf. Accessed 05.11.24, p. 122.

87 Microsoft (2024) *Microsoft Compliance Report – Annex 10 – Windows PC (Operating System) DMA.100160 – Microsoft; DMA.100026 – Microsoft – Operating Systems; DMA.100017 – Microsoft – Online Social Networking Services SECTION 2 Information on compliance with the obligations laid down in Articles 5 to 7 of Regulation (EU) 2022/1925*. https://www.microsoft.com/en-us/legal/compliance/dmacompliance. Accessed 05.11.24, pp. 109-128.

88 The form is public and can be reached under: https://developer.apple.com/support/ios-interoperability/. Accessed 05.11.24.

89 The instructions to the form are not public. It is necessary to have a Google account to reach the form in Android's Issue Tracker system: developer.android.com/dma-interop-request. Accessed 05.11.24.

90 Microsoft (2024), pp. 109-110.

91 The form is public and can be reached under: https://support.microsoft.com/en-us/topic/how-to-submit-a-dma-request-for-windows-data-or-interoperability-1604e103-6c75-40f1-a56f-7fad0fe8ef8a. Accessed 05.11.24.

92 Apple (2024) *Apple Platform Security*. https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf. Accessed

93 Google (2024) *Malware and unwanted software.* https://developers.google.com/search/docs/monitor-debug/security/malware.Accessed 05.11.24.

The comparison above highlights how the three gatekepeers handle interoperability grants. For Apple, integrity factors have the priority on decision making. For the three gatekeepers, notwithstanding the provided documentation for security and integrity regarding the operating system, it is not clear how evaluation and oversight over these requirements will be exercised.

A small detour is necessary to express concerns on Google's presumed compliance with respect to Android. Google stated in its compliance report that due to the open nature of Android, obligations of Art. 6(7) would be automatically fulfilled. However, as the *Google Shopping*[95] and *Google Android*[96] cases have demonstrated, Android is not a completely a FOSS system[97]. It is important to distinguish between the Android system (for which Google has trademarks) and the Android Open Source Project (AOSP), which has a higher number of FOSS components. Only Google-approved forks of AOSP can be called and marketed under *Android* and participate from the benefits of the Android ecosystem, such as software development kits (SDKs) provided by Google[98]. Other forks must be labelled differently. Google remains in control and through a hierarchical organizational structure, code changes to Android eventually need to be approved by Google employees[99]. Ultimately, Google still holds a large degree of discretion over interoperability in Android.

Coming back to Apple, as seen in a previous section, Apple provides broader interoperability policies for its operating system for laptops (MacOS) than for its system for smartphones (iOS). In MacOS, third-party developers have broader access to the hardware and software functions of the device. The two cases below provide further insights.

JIT compilation beyond Safari

The first case relates to restrictions to Just-In-Time (JIT) compilation[100]. JIT compilers improve web performance on iOS. The system also is important for emulators and virtual machines. Without JIT, web content would have to run slower and consume more power. Apple restricts its use to its own browser through strict codesigning requirements[101], only granting the necessary exceptions to the Safari browser[102]. While Apple's Safari uses a sophisticated multi-process architecture for security, third-party browsers are forced to adopt Apple's WebKit model[103], limiting their flexibility in applying their own security measures[104]. The iSH case serves as example of the impact of blocking JIT on emulators. iSH is a FOSS app that emulates the Linux environment on iOS allowing users to access a

94 Microsoft (2024) *How Microsoft identifies malware and potentially unwanted applications*. https://learn.microsoft.com/en-us/defender-xdr/criteria?view=o365-worldwide. Accessed 05.11.24.
95 Case AT.39740 *Google Search (Shopping).* Commission Decision of 27 June 2017.
96 Case AT.40099 *Google Android.* Commission Decision of 18 July 2018.
97 Colomo (2023), pp. 232-245.
98 Krämer J. and Feasey, R. (2021) *Device Neutrality: Openness, Non-Discrimination and Transparency on Mobile Devices for General Internet Access*. CERRE. https://cerre.eu/publications/mobile- devices-net-neutrality-internet-access/. Accessed on 30.10.2024, p. 26.
99 Krämer J. and Feasey, R. (2021), p. 26.
100 JIT compilation is translation (compilation) of source code into binary code during the execution of a program (at run time) rather than before execution. This method makes the program run faster than statically-compiled code that is translated (compiled) prior to deployment. More at: https://en.wikipedia.org/wiki/Just-in-time_compilation. Accessed 05.11.24.
101 Saagar, J. (2020) *Jailed Just-in-Time Compilation on iOS.* https://saagarjha.com/blog/2020/02/23/jailed-just-in-time-compilation-on-ios/. Accessed 30.10.24.
102 See Apple's documentation for JIT: *Protecting code compiled just in time*, available at https://developer.apple.com/documentation/browserenginekit/protecting-code-compiled-just-in-time?language=objc. Accessed 30.10.24.
103 See Apple's documentation for Safari under *BrowserEngineKit*, available at https://developer.apple.com/documentation/browserenginekit?language=objc. Accessed 30.10.24.
104 Open Web Advocacy (2024) *OWA-DMA-Review of Apple's compliance proposal*, v.1. https://open-web-advocacy.org/files/OWA%20-%20DMA%20-%20Review%20of%20Apple's%20Compliance%20Proposal%20-%20v1.0.pdf, p. 37. Accessed 30.10.24.

command-line shell and interact with a suite of traditional Unix tools directly on their iPhones[105]. Although it is currently available on the App Store, in the past Apple has blocked iSH on several occasions[106]. To improve performance and usability, iSH sought access to Apple's JIT compilation APIs, which would significantly enhance execution speeds. Although iOS hardware has long supported JIT, Apple has restricted access to these features, granting them only to its Safari browser, as mentioned before. Given the substantial impact of JIT on performance and battery life, iSH's developers filed a request under Art. 6(7) of the DMA[107]. However, Apple denied the request, arguing that iSH does not meet the criteria under the DMA for browser-related applications and that it does not offer comparable functionality directly on iOS, dismissing iSH's request as outside the scope of DMA interoperability obligations[108].

Apple's denial seems to be based on a narrow interpretation of Art. 6(7) that the interoperability obligation only applies where Apple's own services benefit from the requested functionality in a directly competitive market. In this case, apparently, as Apple does not provide a native terminal emulation environment on iOS, thus does not view itself as competing in the terminal emulation market. From Apple's perspective, this lack of direct competition exempts it from any obligation to extend JIT functionality to iSH or any other non-web browsing applications. This appears to be a strategic denial of interoperability, where a dominant platform is denying access to preserve future competitive advantage[109]. On the other side of the spectrum, in *Android Auto*, the Advocate General expressed the opinion that dominant platforms should ensure interoperability wherever feasible[110]. The AG noted that APIs are essential for ensuring interoperability, and only technical impossibility or significant harm to the platform's operation or economic model would justify a refusal. Recital 57 DMA provides that gatekeepers must provide access to the same features of operating systsem *available* and used by gatekeepers own services. Apple's refusal to grant iSH access to the JIT API appears to lack these objective justifications as the JIT technology infrastructure is already in place for third party browsers and it just needs an extension to non-web browsing applications, like the iSH emulator.

appdb's interoperability request vs Apple's response time

Some FOSS projects have faced delays by Apple in processing their interoperability requests[111]. appdb's request is an example of long waiting time. appdb is an independent, EU-based app marketplace that has allowed iOS users to install and manage apps outside of Apple's App Store for more than one decade[112]. In May 2024, appdb submitted an interoperability request to Apple[113], seeking access to various essential hardware and software functionalities that Apple restricts to its own ecosystem. In July 2024, as Apple had not yet responded, the project communicated to the

105 iSH (2024) *iSH, JIT and EU.* https://ish.app/blog/ish-jit-and-eu. See also, the source code repository at: https://github.com/ish-app/ish. Accessed 30.10.24.

106 Anderson, T. (2020) *Apple cracks down on iOS terminal apps because they can download code.* The Register. https://www.theregister.com/2020/11/09/apple_cracks_down_on_terminal/. Accessed 30.10.2024. See also iSH (2020) *About iSH's pending removal from the App Store*. https://ish.app/blog/app-store-removal. Accessed 30.10.2024.

107 See the full copy of the iSH request for interoperability, available at https://docs.google.com/document/d/1FGE44N7gMwmH31gtZ0hcwKb9xhinu3xSDrjc_d21Qac/edit?tab=t.0#heading=h.ux8o6fgtu07c. Accessed 30.10.2024.

108 iSH (2024) *iSH, JIT and EU.* https://ish.app/blog/ish-jit-and-eu. See also, the source code repository at: https://github.com/ish-app/ish. Accessed 30.10.24.

109 See e.g. Motta, M., Peitz, M. (2024) Denial of interoperability and future first party entry. *International Journal of Industrial Organization.* https://doi.org/10.1016/j.ijindorg.2024.103070. Accessed 05.11.24.

110 CJEU (2024) AG Medina: Google's refusal to provide third-party access to Android Auto platform may be in breach of competition rules. Advocate General's Opinion in Case C-233/23. https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-09/cp240132en.pdf. Accessed 05.11.24.

111 This study got this information by interviewing projects who requested interoperability from Apple but have not publicly disclosed it.

112 See appdb's offcial website, available at https://appdb.to/ and official source code repositories at: https://appdb.to/repos. Accessed on 05.11.24.

113 appdb (2024) *An interoperability request has been submitted.* https://appdb.to/news/530. Accessed 05.11.24.

Commission[114]. As of September 2024, no response from Apple had been given[115]. appdb's request spans several key areas where Apple exercises control, including software signing, push notifications, JIT compilation and access to hardware functions. appdb complains that Apple requires apps to be signed through its Developer Program, creating a dependency on Apple's software signing service. appdb requested that third-party code-signing certificates from trusted authorities be recognized to allow app installations without Apple ID or App Store involvement. appdb also requested to use its own push notification service, a feature currently limited to Apple's paid Developer Program. Like iSH, it also requested JIT compilation access to improve app performance, a capability restricted to Safari and unavailable to non-browser apps. appdb requested interoperability to hardware functions like access to sensors (NFC)[116] and MDM restrictions[117] which have been limited to smaller FOSS projects in the past.

appdb's case relates to complex requests. Longer processing time is expected. Nevertheless, since vertical interoperability direclty impacts the operations of alternatives, effectiveness of Art. 6(7) would also emcompass the timing with which these requests are processed and decided. Unreasonable delays related to core functionality effectively make it difficult for independent developers to provide comparable services.

Refusal to interoperate from a competition law perspective

Until now this study has sought to understand the value of interoperability and the negative impact of gatekeeper power to the detriment of smaller FOSS projects. The sections above highlighted the incentives gatekeepers like Apple may have to resist interoperability and turn the grants ineffective. Freedom to select business partners is a recognised freedom in European jurisprudence, including the right to refuse to deal. The Court of Justice of the European Union (CJEU, the Court) has also acknowledged that in exceptional circumstances, certain behaviors - such as interrupting an established commercial relationship, refusing to initiate new supplies, denying access to crucial inputs or infrastructures, or withholding an intellectual property license - could constitute an abuse of a dominant position, as per Article 102. On the other side, the Commission – as the key enforcer of competition law in the EU – has construed policies in a manner that confines its scope of application of the exceptional circumstances. The latest competition cases in digital markets have relativized discretion to decide when the indispensability condition is applicable and when it is not[118]. This section provides a brief overview of relevant rulings developed by the CJEU relating to interoperability in order to shed light on the limits of denial.

In *Commercial Solvents*[119], the CJEU ruled that a dominant company's refusal to continue supplying a long-standing customer with a key input, essential for the production of a derivative product, amounted to an infringement of Article 82 of the EC Treaty (now Article 102 TFEU)[120]. The Court found that, although the refusal was driven by the dominant company's intention to vertically integrate its operations, this action would have effectively excluded its closest competitor from the downstream market for the drug in question. By doing so, Commercial Solvents would have extended its monopoly

114 appdb (2024) *Recent updates and situation with DMA.* https://appdb.to/news/530. Accessed 05.11.24.
115 See appdb's post on X dated from September 2, 2024: https://x.com/appdb_official/status/1830625907637195153. Accessed 05.11.24.
116 Near-field communication (NFC) is a set of communication protocols that enables communication between two electronic devices over a distance of 4 cm. More at: https://en.wikipedia.org/wiki/Near-field_communication. Accessed 05.11.24.
117 Mobile Device Management (MDM) relates to techniques deployed by IT administrators allowing them to manage and secure mobile devices, including remote installation and configuration controls. More at: https://support.apple.com/guide/deployment/intro-to-apple-device-enrollment-types-dep08f54fcf6/1/web/1.0. Accessed 05.11.24.
118 Colomo (2023), p. 274.
119 Joined Case C-6 and 7/73 *Istituto Chemioterapico Italiano S.p.A. and Commercial Solvents Corporation v Commission of the European Communities*, ECR 223, ECLI:EU:C:1974:18.
120 *Commercial Solvents*, § 23.

into the downstream market[121], undermining the integrity of the competitive process. The Commission and the Court broadened the scope of the principles set out in this ruling to include scenarios where a dominant company holds a vertical relationship with its competitors. In these instances, the dominant company controls access to critical infrastructure, inputs, or other resources that are essential for operating in downstream markets. These resources are considered irreplaceable due to the impracticality of replicating them, either physically or financially[122]. The Court has adopted a cautious approach and interpreted refusal to supply restrictively.

In *Volvo*[123] the Court noted that refusal to supply will only attract Art. 82 if it is accompanied with other abusive practices e.g. imposing unreasonable prices and arbitrary denial to supply. The Court's reasoning was that compelling a company to grant its intellectual property licenses would undermine the core rights of the intellectual property holder, essentially depriving them of the fundamental essence of their intellectual property rights[124].

In *Magill*[125], the Court took a broader view, applying the principles from *Commercial Solvents* to situations where a refusal to grant a copyright license would prevent competition in a downstream market, such as the TV guide market. Magill wanted to publish comprehensive weekly TV guides and needed TV listings information from three TV stations. Each station held a monopoly on its program information. The Court determined that the intellectual property in question (TV listings) was crucial for competing in that market. Although simply holding an intellectual property right does not inherently create a dominant position, the Court recognized that in certain "exceptional circumstances", denying a license to use that right could breach Article 82 of the EC Treaty (now Article 102 TFEU)[126].

In *Bronner*[127], a case concerning refusal to provide access to tangible inputs, the Court clarified the concept of "indispensability" under Article 82 (now Article 102 TFEU). The Court ruled that the party requesting access must demonstrate that no alternative solutions exist, even if less favorable, due to technical, legal, or economic barriers that would make it impossible or unreasonably difficult for competitors to create their own alternatives, potentially in collaboration with others.

In *Microsoft*[128], Microsoft's dominance in the PC operating system market was used to unfairly extend its control over the workgroup server OS market, stifling competition by refusing to disclose interoperability information. Interoperability information was indispensable for competitors to remain viable, and Microsoft's refusal prevented the development of new products, thus harming innovation and consumer choice. The Court rejected Microsoft’s claim that the level of interoperability required by the Commission implied that non-Microsoft server operating systems must replicate all the functionalities of a Windows server operating system. The Court clarified that the Commission’s intention was not for competitors to 'clone' or 'reproduce' Microsoft’s products or specific features of those products[129]. A precedent for this can be found in Directive 2009/24/EC[130], where Article 6 stipulates that, under specific conditions, the authorization of a right holder is not required if the

121 *Commercial Solvents*, § 24

122 Andreangeli, A. (2009) Interoperability as an "Essential Facility" in the Microsoft Case: Encouraging Stifling Competition or Innovation? *European Law Review*, v. 4, pp. 584-611; https://www.pure.ed.ac.uk/ws/portalfiles/portal/14818470/Interoperability_as_an_essential_facility_in_the_microsoft_case_encouraging_competition_or_stifling_innovation.pdf; also Nagy, C., (2007) Refusal to Deal and the Doctrine of Essential Facilities in US and EC Competition Law: A Comparative Perspective and a Proposal for a Workable Analytical Framework. *European Law Review*, v. 32.5, pp. 664-685. https://ssrn.com/abstract=1737710. Accessed 30.10.24.

123 Case C-238/87, *Volvo v Veng*, [1988] ECLI:EU:C:1988:477.

124 *Volvo v Veng*, §§ 8 and 9.

125 Case C-241/91, *RTE and ITP v Commission*, [1995] ECR I-743.

126 Case C-241/91, *RTE and ITP v Commission*, [1995] ECR I-743 §§ 50, 55 and 73.

127 Case C-7/97 *Oscar Bronner v Mediaprint Zeitsung- und Zeitschriftenverlag GmbH & Co. KG and others*, [1998] ECR I-7791.

128 Case T-201/04 *Microsoft v Commission* [2007], ECR II-3601.

129 *Microsoft*, §§ 234, 241, 653 and 657.

130 EU (2024) Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version) (Text with EEA relevance). ELI: http://data.europa.eu/eli/dir/2009/24/oj.

reproduction and translation of code are indispensable for achieving interoperability between independently developed software and other programs. This provision reflects a balance between protecting IP and fostering competition by ensuring that technical barriers do not stifle innovation and market access[131]. *Sony v Datel*[132] reinforced the principle that IP protection is given to the expression of the program (code), but not to its underlying operations or functionalities. Therefore, reproduction or modification of a program for the purpose of achieving compatibility between systems does not necessarily infringe on copyright protections, aligning with Art. 6 of Directive 2009/24/EC.

In comparison with *Microsoft*, it is important to highlight a case faced by Apple before the French Competition Authority (Autorité de la Concurrence) in 2004[133]. *Virgin Mega v Apple* involved Apple's refusal to license its proprietary Fairplay DRM. This technology was key for making Virgin Mega's music downloads compatible with iPods[134]. Virgin Mega argued that Apple's DRM acted as a gatekeeper, preventing interoperability and thus foreclosing competition in the digital music market. The FCA ultimately ruled that Apple's refusal to license was not abusive, as the DRM system was not indispensable for competition, citing alternatives like format conversion and the small percentage of users transferring downloads to portable devices. The FCA analysed the relevant markets related to DRM technologies, portable music players, and downloaded music, finding that Apple did not hold a dominant position in France at the time. Furthermore, the market for portable music players was dynamic, with significant competition from other DRM-protected devices, meaning Apple's dominance in the music player market was not absolute. Apple justified its refusal by arguing that granting access to its DRM could compromise the security of its system, a concern validated by the FCA. Apple's DRM required regular updates to ensure its functionality, and licensing it to third parties would have imposed an ongoing burden, impacting its contractual obligations with the recording industry. *Virgin Mega v Apple* illustrates the complexities involved in mandating interoperability in digital markets. Virgin Mega challenged Apple's refusal to license its Fairplay DRM system, claiming that it restricted competition by preventing compatibility with iPods. However, the FCA ruled that Apple's refusal was not abusive, applying the indispensability test to conclude that interoperability with Apple's DRM was not essential for competition. This decision highlights how regulators weigh the need for interoperability against the protection of proprietary technologies. In contrast to the findings in *Microsoft*, where refusal to disclose interoperability information was deemed an abuse, the FCA found that the existence of alternative means (like format conversion) and strong competition in the market for portable players reduced the necessity for forced interoperability. Back then in 2004, Apple did not have a dominant position in France. In 2024, Apple is a gatekeeper for EU digital markets.

Indeed, the emergence of big tech, allied with the liberalisation of network industries (i.e. telecommunications) made the limits of traditional competition law in the EU become apparent, leading to a paradigm shift in policy and enforcement in the EU. Positive obligations imposed by Commission in cases like *Google Shopping*[135] and *Google Android*[136] required the setting up of an institutional apparatus aimed at profound changes in how companies operate, including altering design of their digital products and business models[137]. A more progressive approach is observed to

131 Recital 15 of Directive 2009/24/EC, *"The unauthorised reproduction, translation, adaptation or transformation of the form of the code in which a copy of a computer program has been made available constitutes an infringement of the exclusive rights of the author. Nevertheless, circumstances may exist when such a reproduction of the code and translation of its form are indispensable to obtain the necessary information to achieve the interoperability of an indepen dently created program with other programs."*

132 Case C-159/23, *Sony Computer Entertainment Europe Ltd v Datel Design and Development Ltd (2024)* ECLI:EU:C:2024:887.

133 Autorité de la concurrence (2004) *9th November 2004: Internet music downloads - The Conseil dismisses VirginMega's complaint against Apple, due to insufficient evidence in view of the case elements available*. https://www.autoritedelaconcurrence.fr/en/communiques-de-presse/9th-november-2004-internet-music-downloads-conseil-dismisses-virginmegas. Accessed 05.11.24.

134 Fried, I. (2005), *Virgin: Apple's not playing fair with iPod.* CNET. https://www.cnet.com/tech/home-entertainment/virgin-apples-not-playing-fair-with-ipod/. Accessed 30.10.24.

135 Case AT.39740 *Google Search (Shopping).* Commission Decision of 27 June 2017.

136 Case AT.40099 *Google Android.* Commission Decision of 18 July 2018.

137 See the conclusions achieved by Colomo (2023), p. 124-152.

remediating abuses derived from new dynamics of digital markets, expanding the scope of Art. 102 TFEU. For instance, the Commission has advanced the idea that dominant undertakings must not only grant access to an essential facility but are under a duty to ensure that such an indispensable infrastructure can accommodate the demands of rivals, both by expanding capacity and by re-allocating existing capacity[138].

As "*[Google's engine's] value lies in its capacity to be open*"[139], the case *Android Auto*[140] serves as another example of gatekeeping control over open instrastructures. In 2018, Google restricted the app's compatibility with Android Auto, a platform allowing apps to be used in cars, arguing that Android Auto was limited to specific app categories to ensure driver safety and platform functionality. The Italian Competition Authority deemed Google's restriction an abuse of dominance, benefitting Google Maps, which offers similar functionality. This decision led to Google's appeal, eventually reaching the CJEU for a preliminary ruling. The CJEU was asked to decide whether Google's denial of interoperation with a company seeking access for its EV charging app constituted abuse. The AG opinion suggested that platforms like Android Auto, which invite third-party integration, should not automatically fall under strict refusal-to-supply criteria. Instead, such platforms could be considered abusive if access limitations unreasonably harm competition and cannot be objectively justified, even without proving indispensability[141]. The AG noted that Google creates value by ensuring that its users have access to a wide variety of interoperable and complementary products and services. It is actually conceived not only to allow but to encourage third-party developers to create versions of their own apps that are compatible with it[142]. In other words, the AG's reasoning stemmed from the fact that Android Auto was designed to foster an ecosystem of third-party apps, distinguishing it from proprietary infrastructure solely reserved for the platform owner's exclusive use. Indeed, scholars have noted that gatekeeprs like Google restrict interoperability to stifle competitors preemptively, leveraging network effects to maintain market control[143]. However, it should be noted that in cases of companies focusing exclusively on proprietary software, like Microsoft in the past and currently Apple, traditional doctrines of essential facilities and refusal to supply would still apply. Bottlenecks caused by their proprietary policies rely on exclusive control over assets.

Freedom of terminal equipment: opening interconnection for internet access devices

The European experience with telecommunications and digital industries in the last decades has consolidated the need for proactive intervention to restore fairer dynamics in markets. Last antitrust decisions suggest gatekeepers have a duty not just to deal with third parties, but to expand capacity to ensure rivals can compete on the relevant market. However, deciding upon which assets and infrastructures from gatekeepers should be subject of interoperability obligations under Art. 6(7) will be a challenge for effective compliance with the DMA. After the functionalities and assets are made open for interconnection, the next step will be connecting them.

Although the gatekeeper interoperability grants contrast with telecommunications due to their complexity, the liberalization of "local loops" granting end-users freedom of choice related to their internet access devices serves as an example of contemporary interoperability regulation in Europe. The discriminatory conduct of gatekeepers in relation to smartphones is in scope similar to that of internet service providers (ISPs) over personal internet access devices. From the telecommunications

138 Colomo (2023), p. 173.
139 Persch, J. (2021) *Google Shopping: The General Court takes its position.* Kluwer Competition Law Blog. https://competitionlawblog.kluwercompetitionlaw.com/2021/11/15/google-shopping-the-general-court-takes-its-position/. Accessed 05.11.24.
140 Case 233/23. *Alphabet and others (Android Auto).* [2024] ECLI:EU:C:2024:694.
141 Case *Android Auto case*, §§ 46 and 47.
142 Case *Android Auto*, § 37.
143 See e.g. Motta, M., Peitz, M., (2024) Denial of interoperability and future first party entry. *International Journal of Industrial Organization*, https://doi.org/10.1016/j.ijindorg.2024.103070. Accessed 30.10.24.

point of view, devices like routers/modems, smartphones, tablets and computers are located at the networks' extremity, making them the primary point for internet access. Akin to the gatekeeper power Apple and Google exercise over smartphones, ISPs can control aspects of routers and modems for internet connection. Despite the absence of monopolies in the European markets among router/modem manufacturers[146], the interconnection between personal equipment and ISPs' networks remains a bottleneck. Gatekeeper control, in this case, comes not from manufacturers but from ISPs. Since network operators can be vertically and horizontally integrated with other internet platforms, they can control diverse elements of the internet value chain[147]. For instance, in Europe, network operators have offered proprietary routers for their subscribers, not authorizing the interconnection of personal routers to the network[148]. ISPs' lock-ins directly affect FOSS, as end-users cannot inspect their firmware or install an alternative operating system[149]. Such limitations became more evident in fiber networks (FTTx), with ISPs alleging security and integrity of the network as excuses to impose their own proprietary devices[150]. This section analyses how telecom regulators and courts in the EU have reacted to network operators' interoperability limitations regarding devices and the network based on assumptions linked to security and integrity.

Freedom of terminal equipment, codified in Art. 3(1) of the Open Internet Regulation - (EU) 2015/2120[151], represents the hardware layer of net neutrality[152]. This regulation transposed into EU the "four freedoms of net neutrality"[153] for end-users giving them agency to choose their content and service providers, internet applications and connection devices. Internet-based communication passes through routers/modems or smartphones. Therefore, having the choice to deploy personal routers/modems enables end-users to remain autonomous in their physical capacity to access the Internet with equipment they trust for security, privacy and sustainability reasons[154]. Indeed, routers are complex devices performing important functions in managing local networks, like WiFi, cloud services, voice over IP (VoIP), TV streaming, port forwarding, dynamic DNS and VPN tunnelling. The vertical integration of ISPs with other content and services providers turn routers/modems into important elements in ISPs' business models[155]. By controlling the access bottleneck, ISPs hold a gatekeeper power imposing their own equipment on consumers with relative flexibility[156]. Such limitations even contrast with the smartphone market, as end-users can freely choose among diverse

146 Directive 2008/63/EC6 aimed to establish competition in the terminal equipment markets. The law requested that Member States withdraw exclusive rights and 'ensure that economic operators have the right to import, market, connect, bring into service and maintain terminal equipment' (Article 3).

147 Marsden, C., Brown, I. (2023) App stores, antitrust and their links to net neutrality: A review of the European policy and academic debate leading to the EU Digital Markets Act. *Internet Policy Review, v.* 12.1. https://policyreview.info/articles/analysis/app-stores-antitrust-net-neutrality-eu- digital-markets-act.

148 See Lasota, L. (2020) Net Neutrality and Free Choice of Routers and Modems in Europe. *JIPITEC*, 11, 303 para 1. https://www.jipitec.eu/jipitec/article/view/288/282. Accessed 30.10.2024.

149 FSFE (2023) *Router Freedom Survey Report – The end-user perspective on freedom of terminal equipment in Europe*. Berlin. https://download.fsfe.org/routers/rf-survey-report-2023.pdf. Accessed 30.11.2024, p. 4.

150 Evidence gathered for this section came from two sources. (i) Documentation provided by regulators and stakeholders during public consultations in diverse regulatory procedures in the EU related to freedom of terminal equipment; (ii) inputs from a survey conducted by the FSFE to collect end-user experience with ISPs in relation to freedom of terminal equipment.

151 Art. 3.1. *End-users shall have the right to access and distribute information and content, use and provide applications and services, and use terminal equipment of their choice, irrespective of the end-user's or provider's location or the location, origin or destination of the information, content, application or service, via their internet access service* (emphasis ours).

152 FSFE (2023) *Stellungnahme der Free Software Foundation Europe e.V. zum "Verfahren über den Erlass einer Allgemeinverfügung zur Abänderung des Netzabschlusspunktes für Passive Optische Glasfasernetze"*. Berlin. https://download.fsfe.org/routers/fsfe-bnetza-fiber-de-2023.pdf. Accessed 30.10.24, p. 8.

153 The 'Four Freedoms' related to the net neutrality policy formalised in the US by the Federal Communications Commission (FCC) in 2005. Marsden, C. (2017) *Network neutrality – from policy to law to regulation*. Manchester University Press, p. 30.

154 Lasota, L., Albers, E. (2023) Making a More Sustainable Telecom Sector with Free Software. In: Jankowski, P., et al (Org.) *Shaping Digital Transformation for a Sustainable Society.* Contributions from Bits & Bäume. Berlin: Technische Universität Berlin. https://publication2023.bits-und-baeume.org/. Accessed on 05.11.2024.

155 Lasota, L. (2020), p. 306.

156 Marsden, C. (2017), p. 2.

models available[157]. In any case, no European ISP has yet met the threshold criteria of the DMA, all remaining subject only to sector-specific telecommunications law.

In 2018, the EECC set rules about the limits of telecom operators' and end-users' networks, tasking national regulatory agencies (NRAs) to determine the position of the "network termination point" (NTP)[158]. Although unrelated to the Open Internet Regulation, the position of the NTP has a direct impact on freedom of terminal equipment. Depending on the location of the NTP, routers and/or modems can belong to ISPs' networks, making them their property instead of consumers'. NRAs were to perform an assessment to determine whether end-users may use their routers and modems. If limitations to this freedom were to be imposed, regulators had to prove the existence of an "objective technological necessity" for the obligatory equipment to be considered part of the ISP network. BEREC was responsible for setting technical guidelines[159] to harmonize the approaches among the regulators. Among the diverse assessment criteria[160], two are relevant for our analysis:

i. Interoperability between the public network and the terminal equipment;

ii. Security of the network.

The three interoperability requirements are[161]:

1. The terminal equipment should comply with the specifications of the network (e.g. standards for DSL, coaxial cable and fiber);

2. Network operators are obliged to make public all necessary specifications to ensure interoperability;

3. Appropriate measures must be in place to enable providers to to protect networks.

In relation to security of the network, BEREC concludes that diversity of devices are positive for security, the number of compromised devices in the event of a vulnerability being discovered in a particular device[162]. Therefore, the security requirements are[163]:

1. End-users should be responsible for proper operation of their equipment and held liable in case of damage caused to the network;

2. End-users need- to ensure that the software used in the equipment does not threaten network security e.g. by using appropriate software only, updating it regularly and using security software. To ensure this the end-user may have support from the equipment vendor;

3. Network operators can take appropriate protection measures against incidents on their networks.

157 BEREC achieves this conclusion by excluding smartphones from the Guidelines on the NTP. See: BEREC (2020) *BEREC Guidelines on Common Approaches to the Identification of the Network Termination Point in different Network Topologies. BoR (20) 46*. https://www.berec.europa.eu/en/document-categories/berec/regulatory-best-practices/guidelines/berec-guidelines-on-common-approaches-to-the-identification-of-the-network-termination-point-in-different-network-topologies. Accessed 30.10.2024, § 144.

158 See Recital 19, Art. 2.9 and Art. 61.7 of the EECC. EU (2018) *Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) (Text with EEA relevance)*. ELI: http://data.europa.eu/eli/dir/2018/1972/oj.

159 BEREC (2020) *BEREC Guidelines on Common Approaches to the Identification of the Network Termination Point in different Network Topologies. BoR (20) 46*. https://www.berec.europa.eu/en/document-categories/berec/regulatory-best-practices/guidelines/berec-guidelines-on-common-approaches-to-the-identification-of-the-network-termination-point-in-different-network-topologies. Accessed 30.10.2024.

160 All criteria consist of: Interoperability between the public network and the terminal equipment; Simplicity of operation; Network security; Data protection; Local traffic; Fixed-line services based on wireless technology. BEREC (2020), p. 11-24.

161 BEREC (2020), §§ 62-69.

162 BEREC (2020), § 95.

163 BEREC (2020), § 91-99.

As BEREC Guidelines are not coercive for NRAs[164], the diverse approaches from regulators have caused a fragmented framework in Europe, creating asymmetries among the interpretations and disproportionately affecting end-users' freedom of choice[165]. The regulatory decisions concerning fiber networks have been the most contradictory. While some countries followed BEREC's assessment criteria (e.g. the Netherlands, Belgium and Greece), others implemented before (e.g. Germany, Finland and Italy). There are countries skipping the guidelines altogether (e.g. Austria, Latvia), and others who have not publicly manifested their positions (e.g. France and Portugal). This study will focus in three countries which have extensively analysed interoperability and security in regards to terminal equipment. The exposition follows a chronological order for the implementation of the respective rules: Germany (2016), the Netherlands (2021) and Belgium (2023).

Germany: fragile evidence against interoperability

Germany was one of the first Member States to implement specific rules for freedom of routers and modems in 2016[166]. The German law encompassed all network topologies by defining the NTP as a socket in the wall, allowing end-users to enjoy freedom of terminal equipment. Interoperability was mandated by requiring operators to allow interconection with end-users devices meeting basic standards of the country telecommunications legislation. Operators were required to publish and regularly update the technical documentation for interface connection[167]. In 2023, the German regulator, Bundesnetzagentur, opened procedures to analyse a request made by fiber operators to limit freedom of terminal equipment for fiber networks[168]. Operators claimed, among other things, issues of security of the network and of interoperability. The German regulator has analysed the case applying the BEREC Guidelines on the NTP. Although by the time of this study no official decision was made, the regulator published a draft decision. No "objective technological necessity" was found to limit freedom of terminal equipment for fiber networks[169]. Among the diverse conclusions achieved by the regulator, the following are relevant for this study:

- **Interfaces should be public and well documented**. Although operators claimed that interfaces for interconnection could not be sufficiently described to avoid vulnerabilities, the regulator confronted the allegation affirming that there is a wide range of mechanisms for error prevention and interoperability testing. The regulator emphasized that telecommunications infrastructure should not be a "black box" with only partially known properties[170];

- **Fragile evidence against interoperability**. Confronting the operators' request to install testing requirements and to limit device freedom based on disruption risks for the network due to interoperability issues, Bundesnetzagentur affirmed that it has received very few reports of disruptions. There was one case in 2016 that remained as an isolated one. The

164 While NRAs "must have taken utmost account" of BEREC decisions, EECC has not set any legal requirement for them to follow.

165 Godlovitch, I., et al (2023), pp. 6-7 and Lasota (2020), pp. 309-312.

166 Germany (2016) *Gesetz zur Auswahl und zum Anschluss von Telekommunikationsendgeräten*. http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl116s0106.pdf. Accessed 30.10.24.

167 See e.g. Deutsche Telekom (2023) *Technical Specification of the Broadband-Access-Interfaces in the Network of Deutsche Telekom*. 1 TR 112, v. 14.1. https://www.telekom.de/hilfe/geraete-zubehoer/telefone-und-anlagen/informationen-zu-telefonanlagen/schnittstellenbeschreibungen-fuer-hersteller. Accessed 30.10.2024.

168 Bundesnetzagentur (2023) *Verfahren über den Erlass einer Allgemeinverfügung zur Abänderung des Netzabschlusspunktes für Passive Optische Glasfasernetze*. https://www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/Unternehmenspflichten/Schnittstelle_netzabschluss/start.html. Accessed 30.10.24.

169 Bundesnetzagentur (2024) Entscheidungsentwurf zu einem Antrag auf Erlass einer Allgemeinverfügung nach § 73 Absatz 2 TKG zur Abänderung des Netzabschlusspunktes für Passive Optische Glasfasernetze. https://www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/Unternehmenspflichten/Schnittstelle_netzabschluss/entscheidungsentwurf.pdf. Accessed 30.10.24.

170 Bundesnetzagentur (2024), p. 19.

regulator found surprising the lack of documented disruptions considering the operators are present internationally in various markets[171];

- **Theoretical disruptive scenarios are not enough for limiting interoperability**. The regulator questioned the far-reaching security scenarios posed by operators, claiming the lack of objectivity in the reports. Although the described scenarios could never be completely ruled out, the proposed intensive testing goes beyond what is legally justifiable to limit interoperability[172];

- **Security risks are overstated**. Bundesnetzagentur rebutted operators by demonstrating that past records have shown that operators' proprietary devices were also security vulnerable. Software updates provided by the manufacturers are unlikely to reach end-users using auto-updates slower than operators' devices[173]. The regulator also rejected the assumption that the only way to avoid vulnerabilities is to avoid freedom of terminal equipment altogether by assigning unchangeable and unique identifiers to the devices[174].

The Netherlands: interoperability should be provided quickly and effectively

In 2021, the Dutch Authority for Consumers and Markets (ACM) published its decision regulating freedom of terminal equipment in the country based on the BEREC Guidelines on the NTP[175]. The regulator follows BEREC by stating that freedom of routers and modems is important for markets and end-users: while competition and innovation are promoted among router manufacturers, it lowers the switching costs for end-users and increases their security[176]. The regulator has not found any "objective technological necessity" to limit interoperability among end-users devices and the ISPs' networks[177]. Among the several arguments put forward, the following are relevant for this study:

- **Interfaces should be publicly and sufficiently documented.** Interface specifications should be sufficient for manufacturers to develop a terminal device that is interoperable with the ISPs' networks. The specifications published should enable suppliers and/or manufacturers to create configuration files, including the encrpytion methods used in the connection[178];

- **Interoperability should be provided quickly**. End-users should not wait more than one month in the queue to have the connection established with their own equipment. Operators can reasonably charge end-users in case of additional costs to make the interconnection work[179]. Operators must publish all specifications not only for manufacturers, but also instructions for end-users to configure the terminal equipment they have connected themselves to the network, including security credentials[180];

- **No self-preferencing regarding security**. Operators should not self-prefer devices on security allegations. Operators are allowed to set reasonable security standards in their technical specifications, as long as they apply the specifications to themselves, including: password, authentication and encryption standards; provision of ports not compromising integrity of the network; authentication of software installed in the devices[181];

171 Bundesnetzagentur (2024), p. 26.
172 Bundesnetzagentur (2024), pp. 33 and 36.
173 Bundesnetzagentur (2024), p. 52.
174 Bundesnetzagentur (2024), p. 49.
175 ACM (2021) *Beleidsregel handhaving besluit eindapparaten (bepaling van het netwerkaansluitpunt en de vrije keuze van eindapparaten) Markten goed laten werken voor mensen en bedrijven Zaaknr. ACM/19/036305 / Documentnr. ACM/UIT/558439*. https://www.acm.nl/system/files/documents/beleidsregel-handhaving-besluit-eindapparaten.pdf. Accessed 30.10.24.
176 ACM (2021), p. 5.
177 ACM (2021), p. 9.
178 ACM (2021), p. 13.
179 ACM (2021), p. 14.
180 ACM (2021), p. 12.
181 ACM (2021), p. 18.

- **Equipment security is responsibility of the end-user**. Freedom of terminal equipment also means that the end-user is responsible for its correct functioning. This does not apply if the device has been provided and managed by the operator. Generally security issues are not expected if the end-user regularly updates the router's firmware and applies security best practices[182].

Belgium: end-users should be educated about interoperability

In September 2023, the Belgian Institute for Postal Services and Telecommunications (BIPT) published its decision on the location of the NTP in compliance with the BEREC guidelines[183], regulating freedom of terminal equipment in the country. Routers and modems are not considered to be part of the ISPs' infrastructure, opening up the market for end-users. The regulatory decision encompassed fiber networks. Differently from the other examples listed in this study, the regulator's decision was questioned by Orange - a Belgian operator - in court[184]. In *Orange Belgium NV v BIPT* the operator claimed lack of diligence from the regulator in analysing the existence of "objective technological necessity" to limit freedom of terminal equipment in fiber networks. For Orange, the topologies of the Belgian networks differ from other countries in a way that fiber router/modems should pertain to ISPs, not end-users[185]. The court dismissed all claims from Orange, confirming BIPT's regulatory assessment to open the router market due to the absence of objective technological necessities to limit freedom of terminal equipment[186].

In its regulatory decision, BIPT stated that end-users should not be obliged to use operators' routers. ISPs should not perform the decision for end-users regarding their choice of using personal routers and modems[187]. Instead, similarly to smartphones, routers and modems should pertain to end-users and be able to be reused on different networks with the same technology[188]. Among the diverse arguments BIPT listed for interoperability and security, the following are relevant for this study:

- **Interoperability incurs in low risks for the operators.** Rebutting the allegation from operators that possible network disruptions would outweigh the benefits for the end-users, BIPT highlighted the fact that no significant problems have yet occurred at the network level. The various operators responding to the correspondent public consultations were not able to mention any specific case[189];

- **End-users should be educated about interoperability**. Notwithstanding the learning curve involved in using personal routers for internet connection, BIPT assumes that the interested customer will inform himself about the adverse effects and costs one may experience. Operators can play a useful role by publishing information in a clear manner that supports end-users as much as possible in installing their own modem. The better the operators inform their customers about this, the fewer problems that end-user will have lowering the operational costs for the operators[190];

- **Openness benefits security**. BIPT noted that in several Member States network operators use standard security protocols, whereby necessary information is publicly available. As long as the software running on end-users' routers complies with open specifications interoperability

182 ACM (2021), p. 17.
183 BIPT (2023) *Decision of 26 september 2023 regarding the identification of the network termination point for broadband services*. Accessed 30.10.24.
184 *Orange Belgium NV v Belgish Instituut voor Postdiensten en Telecommunicatie (BIPT).* Arrest. Hof van beroep Brussel. Sectie Marktenhof 19 Kamer A. 2023/AR/1529. https://www.bipt.be/consumers/publication/judgement-of-the-market-court-of-22-may-2024-appeal-by-orange-belgium. Accessed 30.10.24.
185 *Orange Belgium NV v Belgish Instituut voor Postdiensten en Telecommunicatie (BIPT),* p. 8
186 *Orange Belgium NV v Belgish Instituut voor Postdiensten en Telecommunicatie (BIPT),* p. 39.
187 BIPT (2023), § 85.4.
188 BIPT (2023), § 85.5.
189 BIPT (2023), § 111.
190 BIPT (2023), § 107.

should be provided. Open and public discussion about the necessary level of security for the networks ultimately improves the security standards[191].

Notwithstanding the fragmented regulatory framework in Europe for freedom of terminal equipment, this section exposed a high level of awareness among telecom regulators. Operators' security arguments were balanced against the benefits of interoperability. The stiff disputes in relation to router/modem freedom in fiber networks made explicit the necessity to properly balance the overstated risks of network security in limiting interoperability of personal equipment. Ultimately the liberalisation of router markets becomes aligned with open internet and device neutrality imperatives.

Conclusion and future research

The conclusions of the different cases, contexts and regulatory frameworks in this study converge to one aspect: effective interoperability requires institutional arrangements that give primacy to collective forms of sustainable and persistent access, use and reuse of assets allowing fair competition[192]. FOSS, in similar fashion to unseen physical public infrastructure, handles many of the digital world's services, including those unseen by end-users. Business and consumers rely on digital systems for communications, financial transactions, transportation, healthcare, and other vital services and many of those digital systems rely on FOSS. Interoperability is key for keeping this vital ecosystem running[193]. DMA represents a leap forward in comparison with how traditional competition law has dealt with market failures. Art. 6(7) and Art. 6(4) put vertical interoperability in the core of this new regulatory venture. The effective implementation of these obligations will require substantial investments from gatekeepers and significant compliance efforts from the Commission over time.

Interoperability cannot be treated as an one-off target. Analysing Apple's gatekeeper status clearly shows how the viability of alternative solutions depending on gatekeepers' infrastructures to reach end-users will demand strict attention from the Commission to DMA's postulates. Openness of software translates into collective forms of sustainable and persistent access, use and distribution of source code. Ensuring a level playing field for FOSS translates into DMA enforcement policies focusing on functional needs of FOSS developers interacting with gatekeepers. Remedies provided in compliance with Art. 6(7) should minimise dependencies on proprietary technologies, standards and protocols involving further licensing schemes against the DMA's free-of-charge requirements. Enforcement should consider open standards, specifications, protocols and formats, taking due account of the coverage of functional needs, maturity and market support and innovation. When necessary, intellectual property rights licensed on fair, reasonable and non-discriminatory (FRAND) terms should consider the implementation not only for proprietary business users but also to be compatible with FOSS licenses on a royalty-free basis.

Antitrust decisions in the EU have implied a duty to deal on non-discriminatory terms and conditions and, more generally, the existence of a principle of equal treatment. Network industries have relied on FRAND licensing schemes for granting access. In the software industry, FRAND licensing is sometimes at odds with FOSS[194]. Normally FRAND terms includes the expectation that there will be

191 BIPT (2023), § 179.

192 See e.g. the opinion of the recent Commissioner Henna Virkkunen prioritizing DMA enforcement efforts to *1) to open up closed ecosystems, be it in operating systems, web browsers or online marketplaces; 2) to give consumers choice and the ability to take back control in an environment where they feel large digital companies are powerful, and 3) to ensure that data belongs to those who generate it and not to those who can best exploit it*. Virkkunen, H. (2024) *Questionnaires to the Commissioners-designate Henna Virkkunen Executive Vice-President for Tech Sovereignty, Security and Democracy*. https://hearings.elections.europa.eu/documents/virkkunen/virkkunen_writtenquestionsandanswers_en.pdf. Accessed 07.11.24.

193 See e.g. the comprehensive report by Scott, S., et al (2023) *Avoiding the success trap: Toward policy for open-source software as infrastructure*. https://www.atlanticcouncil.org/in-depth-research-reports/report/open-source-software-as-infrastructure/. Accessed 05.11.24.

194 See e.g. Phipps, S. (2019) *Open Source and FRAND: Why Legal Issues Are The Wrong Lens*. Open Forum Europe. https://openforumeurope.org/publications/release-of-opinion-paper-on-open-source-and-frand-by-ofa-fellow-simon-phipps/. Accessed 05.11.24.

multiple, negotiated, bilateral relationships between patent owners and code users. FOSS licensing regimes do not include side-tracks but provide universal grants. FRAND assumes the possibility of further negotiations over royalty-based licensing. FOSS licensing is automatic without the need for further authorisations or concessions. The "free-of-charge" obligation of Art. 6(7) has the potential to encourage solutions based on open standards[195] with FOSS projects in the lead.

In contexts related to gatekeepers' request-driven compliance approach to Art. 6(7), further specification from Commission is a welcomed initiative. The lessons learned in the telecom sector serve as examples to manage expectations for opening up infrastructures and assets under monopolistic control.

The conclusions of this study necessarily have limitations. Evaluation and comparison of interoperability solutions implemented in the context of DMA related to FOSS are still scarce in the literature. Sources of information, evidence, inputs and insights were collected during stakeholder mapping, interviews, bilateral and multi-lateral meetings. The relatively small number of available cases and contexts related to FOSS linked in this study reflects the challenges in accessing publicly available information free from confidentiality restrictions. Content related to merits, procedures and outcome of the interoperability requests under Art. 6(7) is still not easily available. Therefore, follow-up research should be performed when more information becomes available for academic scrutiny. Specifically, the Commission's specification procedures will serve as logical next step, as it will shed light on concrete recomendations for achieving effective interoperability.

Ackowledgements

This study relied on the invaluable contribution of several people. The authors thank Melina Braun, Mariam Sattorow, Marc Prud'hommeaux, Hans-Christoph Steiner, Siguza, Marc Stibane and Florian Snow for their crucial help in the course of the investigation. The authors are truly grateful for reviews, comments and feedback received at the Article 19 Syposium "DMA enforcement: Trends and gaps in the first year of application". The authors also sincerely appreciate the meticulous proofreading of Richard Schmeidler. Any inconsistency and imprecision are the responsibility solely of the authors.

Declaration of conflict of interests

The FSFE is intervening in Apple v Commission (T-1080/23). This study does not focus on Apple's litigation actions and FSFE's intervention as mentioned in p. 8.

As an independent non-profit organisation, the Free Software Foundation Europe has received corporate donations from some of the gatekeepers (https://fsfe.org/donate/thankgnus.html) among other companies and individuals. The FSFE receives no donation higher than 20% of its yearly budget. No funding was received specifically for this study.

195 Open standards are not as a binary complement of proprietary standards but instead there is a spectrum from completely closed to completely open. The openness of a standard can be assessed based on criteria related to procedural transparency, community, democracy, costs, freedoms and permissions, and restrictions. See e.g. DeNardis, L. (Org.) (2011) *Opening Standards the Global Politics of Interoperability*. MIT Press.