Apple's response to the consultation
on the first review of the Digital Markets Act

September 24, 2025

Summary of Apple's recommendations

1. The DMA should be repealed while a more appropriate fit for purpose legislative instrument is put in place.

2. If the DMA is not repealed:

   I. Enforcement should be undertaken by an independent European agency, separate from the European Commission, shielded from political interference, and able to ensure a predictable, equitable, balanced, and text-based application of the DMA that respects fundamental rights.

   II. The DMA enforcement authority should be obliged to involve the relevant EU independent agencies for data protection and cybersecurity where it is considering any action which could impinge on the fundamental right to privacy or on end users' online security.

   III. The notion of "effective compliance" must be clarified to mean allowing end users and business users to exercise their rights under the DMA. The uptake rate of those rights should not and cannot serve as a valid measure of compliance.

   IV. Gatekeepers should be precluded from exercising DMA related rights on the same basis as gatekeepers are excluded from exercising rights under the Data Act.

   V. The DMA should include an overarching proportionality test that explicitly requires the EC to consider the interest of end users, including safety, security, privacy, integrity, and innovation. It should also acknowledge the importance of the fundamental rights of gatekeepers, such as intellectual property rights and the right to conduct their businesses, including through product differentiation. The DMA's enforcement should not sacrifice those objectives for the benefit of technology companies' unfettered access to users and their data.

   VI. Articles 5(4), 6(3), and 6(7) should be repealed or completely overhauled. Article 6(4) should be overhauled. These obligations—exacerbated by their interpretation by the EC—have caused the most harm to EU consumers and will continue to do so, without any offsetting benefits.

VII. Apple has also made a number of other specific suggestions in relation to the text of several DMA articles in light of actual experience which has demonstrated serious deficiencies.

(1) At Apple, our mission is to create and share technology that empowers people and enriches their lives. We do that by making products and services that are intuitive and simple to use, that work seamlessly together, that protect people's privacy and security, and that provide a trusted, quality experience our users love. We recognize consumers have many options to choose from, and we compete by offering them an experience on our products that is distinctly Apple.

(2) The European Commission's use of the Digital Markets Act to redesign our products has had a real impact on our users. The EC's extreme interpretations of the law have created new vulnerabilities for our users and a degraded experience, including:

(i) *Privacy and security:* We know our users choose Apple in part because of our promise to do everything we can to protect their privacy and security. However, the sad truth today is that our users in Europe are subject to more threats than ever before as a result of the EC's approach to DMA enforcement against Apple.[1] The EC effectively treats the privacy and security of European users as irrelevant factors. For example, the EC has forced Apple to allow companies to collect sensitive user data that today, even Apple can't access—including the complete content of their notifications on iOS and a full history of their Wi-Fi passwords. This is some of the most sensitive information available on an EU user's iPhone, and it undermines the principles that motivate the EU's General Data Protection Regulation.

---

[1] *See, e.g.*, European Centre for International Political Economy, The EU's Digital Markets Act: A Gift to Hackers - and a threat to Competition, 2025 ("*[…]the European Commission is prioritising regulatory mandates over the integrity of established security architectures, potentially exposing users to heightened cybersecurity risks. The unintended consequences of this policy not only expose citizens to greater cybersecurity threats but could also reduce competition in the mobile ecosystem space rather than enhance it")*. *See also* European Centre for International Political Economy, Cybersecurity at risk: How the EU's Digital Markets Act Could Undermine Security across Mobile Operating Systems*, 2025* (*"[t]he DMA focuses on market structure, overlooking how differences in operating system design affect security vulnerabilities. A one-size-fits-all approach ignores platform-specific security needs, leaving European users exposed to cyber threats. This risks undermining the EU's economic security agenda, including initiatives like the Cybersecurity Strategy, Cyber Resilience Act, and NIS2 Directive, which aim to strengthen digital defences")*. *See also* Chamber of Progress, New Campaign: How Digital Markets Act Has Become Europe's Digital Curtain, 2025 ("*[t]he forced modularity mandated by the DMA has created security gaps and exposed users to greater fraud and cybersecurity threats. The introduction of third-party app stores and sideloading has created new vectors for malware and bad actors, potentially compromising user data").*

(ii) *A widening gap between the EU and the rest of the world:* Our users in Europe expect that Apple will bring new features, technologies and experiences to market every year. Apple's relentless focus on innovation year after year is a critical aspect of its success. This is no easy task. Apple is working on some of the most complicated and sophisticated engineering and design challenges in the world. The EC's radical interpretations of the DMA has made it nearly impossible for Apple to bring some of these new features to Europe.

The EC has forced Apple to delay new features in the EU, leading our users' experience in the EU to lag behind the rest of the world. To date, those delayed features include Live Translation, iPhone Mirroring, and Visited Places and Preferred Routes on Maps. These delays have a number of causes—including privacy and security concerns, as well as the intensive engineering work required to bring Apple features to competitors' products.

(iii) *Undermining Trust:* Apple revolutionized software distribution in 2008 when it first introduced the App Store. Apple offered users an alternative to the chaos of the Internet. It created a marketplace that is more secure, more seamless, and more trusted than any other. The EC has used the DMA to create a more complicated, less trustworthy experience that introduces totally new threats to our users. It has opened the door wider for scams and malware, and brought new categories of apps to iPhone—like pornography—that Apple has never allowed and that expose children to new risks.

(3) Apple still offers European consumers the very best products in the market—from cutting edge design and quality to a user-centric approach to security and privacy. However there is no question that the experience in Europe has been diminished by the EC's actions—as a result our users confront increased privacy and security risks, delays to new features, and a more fragmented, less seamless experience on our products. The experience for our European users is not the best we can do because of the EC's mandates.

(4) We worry this is only the beginning. Our EU users' experience on Apple products is already falling behind the rest of the world because of the EC's approach to the DMA. The gap between our products in Europe and our products in the rest of the world is only growing with each passing day. In the future, it may not be possible to share some products and features in the EU at all—especially in fast-moving areas like artificial intelligence. This is not Apple's choice. It is not what is best for our European users.[2] But it is what the EC has mandated.

---

[2] *See, e.g.*, Disruptive Competition Project, Digital Markets Act Enforcement at a Crossroads: Avoiding Overreach and Ensuring Progress, 2024 ("*[i]f Europeans only have access to second best, or even worse, then this will accelerate the already growing gap in tech adoption in Europe compared to other global economies. If we want to boost our competitiveness, hampering our ability to compete is not the solution. Forcing our businesses to build with limitations simply won't lead to ambitious growth"*).

(5) The EC's enforcement efforts are targeting some of the key reasons people choose Apple products—including the privacy and security protections, and the simple, seamless and intuitive experience they offer right out of the box. The EC is using the DMA to remove a choice from the market—because European consumers cannot get the same, distinctly Apple experience we offer in the rest of the world.[3]

(6) The EC's approach to DMA enforcement against Apple has ignored the interests of our users in favor of a myopic focus on the commercial interests of a handful of large, already successful, developers. The EC has encouraged companies to weaponize the law to benefit themselves: to collect more sensitive user data, to force Apple to share our IP for free, and to delay Apple's ability to share new features and products.[4] The EC's enforcement approach is inexorably driving Apple products to be more like our competitors'—denying European consumers the distinctly Apple experience they expect, at the same high bar we offer in the rest of the world.

---

3 *See, e.g.*, Chamber of Progress, New Campaign: How Digital Markets Act Has Become Europe's Digital Curtain, 2025 ("*[t]he regulatory uncertainty surrounding the DMA has led to significant delays in the rollout of cutting-edge technologies in Europe. From AI-powered features to new social media platforms, European users are increasingly finding themselves behind the global curve in accessing the latest digital innovations. In some cases, companies have been forced to remove features entirely from their European offerings to comply with the DMA, leaving EU consumers without important innovations compared to their global counterparts*").

4 *See, e.g.*, Pablo Ibáñez Colomo, The Draft Digital Markets Act: A Legal and Institutional Analysis, Journal of European Competition Law & Practice, Vol. 12, issue 7, 2021 (*"the greater leeway the authority enjoys under the Draft DMA can be expected to increase firms' incentives to influence regulatory outcomes. […] Similarly, the potentially far-reaching scope of intervention under Articles 5 and 6 and the absence of apparent constraints could be exploited by potential beneficiaries, in the sense that they would have a clear incentive to seek an expansive interpretation of the relevant provision"*).

(7) *Different rules for different companies.* The EC has focused its enforcement efforts almost entirely on Apple. Apple has been targeted by the EC five times—more than every other company combined. The EC has also moved much more quickly to bring decisions against Apple. Investigations of other gatekeepers languish while the EC has pursued its campaign to redesign the iPhone. And it levied an unprecedented fine for alleged non-compliance with a provision of the law while holding Google and Booking.com to very different standards under the same provision.[5] This biased enforcement has no legitimate basis—Apple is not the market leader in the EU. Samsung is, and Chinese manufacturers are swiftly catching up. The DMA has actually given a leg up to the market leaders, while singling out an American company with onerous rules.

(8) *Ever-shifting interpretations of the law.* Apple has sought to comply with the text of the DMA. Time and time again, the EC has focused on what it characterizes as the "spirit" of the law. We were the first and only company to announce a comprehensive compliance plan in January 2024, 3 months before the compliance date. We engaged earnestly and genuinely with the EC at all opportunities, holding over 200 meetings over this time. But instead what we have found is constantly moving goalposts that appear to only apply to Apple.

(9) The EC's outcome-focused interpretations have shifted significantly over time as they respond to a group of powerful, vested interests.[6] The EC has used the threat of punitive fines to force Apple to make concessions that benefit a handful of developers at the expense of the user. The lack of meaningful and effective judicial review has only exacerbated the problem.

---

5 *See, e.g.*, Jasper van den Boom, Procedures in the DMA: non-compliance navigation – Exploring the European Commission's space for discretion and informality in procedure and decision-making in the Digital Markets Act, European Competition Journal, 2025 ("*[t]he Commission is not completely beyond limits in exercising its discretion: It has to respect the interest of the Union, must not make manifest errors of appraisal or misuse of power In extreme cases, some kind of limit could stem from the principle of equal treatment – if the Commission goes fiercely against Apple, but does not investigate the same behaviour from Microsoft, this may give rise to irritation and, legally speaking, issues of equality before the law (Art. 20, 21 Charter of Fundamental Rights) when it amounts to a tangible discrimination"*).

6 *See, e.g.*, Chamber of Progress, The Digital Markets Act's "Statler & Waldorf" Problem, 2024 ("*[i]t wasn't consumers or European citizens who clamored for the Digital Markets Act — it was mostly "middleman" services that hoped to get better placement on iPhones and Android devices, in app stores, or in Google search results. Content aggregators like Yelp, Tripadvisor, and Booking.com. Big app makers like Spotify, Epic Games, and Match.com. Rival search engines like Ecosia, Yandex, and DuckDuckGo. The companies largely achieved their results: a law that bans big tech services from vertically integrating their services—even if those integrations help consumers*"). *See also* Computer & Communications Industry Association, "New Study Finds DMA Procedural Flaws Hinder Compliance and Enforcement, Proposes Fixes Ahead of Review," 2025 ("*[t]he back-and-forth between gatekeepers and access seekers, as well as subsequent arbitration by the European Commission, is noticeably opaque. The Commission's goalposts also keep shifting, making effective compliance extremely difficult*").

(10) *Enabling copying and theft of intellectual property.* Apple is widely regarded as one of America's—and the world's—leading innovators. We create unique experiences unlike any other in the market. The EC has weaponized the DMA to require Apple to share our proprietary technology and features with our competitors—by granting any request they make, however expensive, time-consuming, or proprietary. The EC has consistently ignored Apple's intellectual property rights in its rush to force Apple to redesign its products to benefit third parties. The EC has even suggested that Apple share our plans for new features and products with our competitors, months or years ahead of sharing them with our users. Requiring companies to give away their innovations for free and disclose their product roadmaps poses an existential threat to competition and undermines incentives to introduce new innovations in the EU.[7]

(11) The EC has caused serious harm to Apple users and digital markets in the EU. If the EC continues on this course, the damage will likely only get worse. So it's critical that European consumers and Apple users are put at the center of this review process, in order to make a fair evaluation of the DMA's impacts—now and in the future.

(12) The most effective way to repair the damage and prevent further harm would be a repeal of the law. At a minimum, we urge a repeal of specific provisions including Articles 6(7), 6(4), 5(4) and 6(3). Apple does not make this request casually. Unfortunately it sees little choice given the experience of the last three years. The amendments are needed to address the EC's disregard of the text of these provisions. There is no other way to ensure that the law is not further misused by the EC's aggressive outcome-focused interpretation of the law that favors a few special interests at the expense of the European consumer.

(13) We also set out a non-exhaustive list of other potential changes that could address ambiguity in the text, discriminatory enforcement, and procedural shortcomings that have exacerbated its negative impact. These measures include, for example, introducing an overarching proportionality test that explicitly requires the EC to consider the interests of end users, as well as the fundamental rights of gatekeepers, such as intellectual property rights and the right to conduct their

---

[7] *See, e.g.*, Information Technology and Innovation Foundation, Six Ways the DMA is Backfiring on Europe by Harming Users, Innovation, and Allies, 2025 (*"[a]nticipatory regulation creates uncertainty, delays innovation, and reduces platforms' incentives to invest in new features and services"*). *See also* Carmelo Cennamo et al., Digital Platforms Regulation: An Innovation-Centric View of the EU's Digital Markets Act, Journal of European Competition Law & Practice, 2023, Vol. 14, No. 1, 2023 ("*[t]he DMA seems to implicitly assume that data can be created, accessed, or used at zero cost* (…) *producing new data out of novel interactions requires important investments* (…) *data need to be transformed into valuable insights via aggregation and combination with other data via the use of models, tools, and organisational resources (…)* [this] *may jeopardise the platform provider's incentives to make the necessary investments to generate novel and valuable (for all ecosystem participants) data*").

business, including through product differentiation. These changes may mitigate some of the harms but they will not be as effective as repeal.

(14) Apple calls for a fundamental review as to whether the European Commission meets the criteria of an independent authority in the context of DMA enforcement. The EC has been highly responsive to external pressures—even going so far as to encourage complaints and work hand-in-hand with third-parties to support their campaign against Apple and its users.[8] The DMA should be a technical instrument, applied by technical experts in a proportionate manner and strictly aligned with the legislative text. Judicial review is no substitute for impartial enforcement. Given the fast-moving nature of digital markets, combined with the absence of suspensory effects of an appeal, any corrective measures at the judicial level several years after decisions have been implemented will inevitably come too late. Enforcement should be undertaken by an independent agency, shielded from political interference and able to ensure a fair, balanced, and text-based application of the DMA.

I. The EC's DMA enforcement has harmed Europeans

(15) The interests of end users—their privacy, security, and experience—are being sacrificed to the short term benefit of a few commercial interests. The EC has undermined consumer protection, data privacy, child safety, and other core European values.

(16) **Balancing Access with Privacy, Security, and Product Integrity**. Interoperability with mobile operating systems requires careful and thoughtful engineering.[9] Exposing sensitive hardware and software functionalities and providing access to on-device data creates security vulnerabilities and increases privacy and security risks. Safe interoperability solutions—which are a foundational part of Apple's promise to users—often require user permissions, sandboxing, authentication, and

---

8 *See, e.g.*, King & Spalding, The Digital Markets Act - A procedural journey towards effective compliance (report commissioned by Computer & Communications Industry Association), 2025 ("*the third-party consultation process [is] a "black box", with little clarity on how the Commission interacts with third-parties. Accordingly, there may be a danger that the Commission could end up consulting an insufficiently balanced cohort of players to the benefit of only the most activist business users*").

9 Apple invests significant resources in providing developers with the tools, technologies, and services for developing innovative apps and hardware for Apple's operating systems. Apple has long embraced interoperability when it is able to do so from a technical perspective, and where it is safe, secure, and privacy-friendly. To that end, Apple provides an extensive and continuously evolving set of proprietary, IP-protected technologies, tools, and services —including over 250,000 application programming interfaces ("**APIs**")—that enable developers to integrate their apps with Apple's hardware and software. These technologies, tools, and services span a wide range of capabilities, such as machine learning, augmented reality, health and fitness, widgets and live activities, spatial computing, user interactions, and high-performance graphics. With each platform release, Apple expands and refines its technologies, tools and services to assist developers in bringing their ideas to life and delivering rich, responsive, and optimized experiences across Apple platforms. Apple is also a contributing member of over 100 standards organizations that drive interoperability and compatibility.

granular and revocable consent over data access. For example, Apple's users expect that third-party developers cannot simply track their location using the iPhone's GPS, or spy on them using its camera without their explicit consent.

(17) The EC has embraced a discriminatory and extreme interpretation of Article 6(7). It has used this article to force Apple, and Apple alone, to redesign its operating system in ways that will undermine security, privacy and the integrity of the device.

(18) First, the EC decided that privacy and security are not relevant considerations for designing interoperability solutions. The EC has forced Apple to remove safeguards, leaving the protection of privacy and data security almost entirely to the discretion of third party developers. For example, in its specification decision in relation to connected devices, the EC decided that Apple can no longer guarantee end-to-end encryption of iOS notifications between the originating server and the target device. The EC required Apple to redesign iOS to allow decryption of the notification before transferring it to the connected device, enabling the developer's companion app to manipulate it. The EC ignored the potential that developers could intercept previously-encrypted messages to collect user data for online advertising or other purposes.

(19) Second, the EC prevents Apple from restricting interoperability solutions to specific, well-defined use cases. Apple's Exposure Notifications framework illustrates the dangers here. In 2020, Apple enabled specific iOS apps to track proximity of nearby devices, to inform people of potential exposure to COVID-19. A register of all other devices that a user encounters is obviously extraordinarily sensitive data, and so Apple imposed strict restrictions on its use—including limiting which apps are entitled to access it. Apple did not even make the API available to other product teams within Apple. But the EC's use case agnostic principle would, if applied as it intends, require opening this API, for example, to providers of social networks or online ad services, which would allow them to create social graphs without the user's knowledge. The EC's interpretation of Article 6(7) is that the privacy and security of our users cannot be taken into account by Apple when considering a request for interoperability.

(20) The EC has weakened Apple's ability to protect European consumers from bad actors, irresponsible data traders, or accidental misuse of iOS functionalities. The EC's misguided approach collides with the expectation of millions of European consumers who opt for Apple products precisely because of the trust they place in Apple's commitment to privacy, security, and safety.

(21) **Alternative Distribution Undermines Privacy and Security**. The DMA eliminated a core part of Apple's security architecture by requiring Apple to allow the distribution of apps outside of the App Store. This prevents Apple from monitoring apps on an ongoing basis to protect against threats for end user privacy and

security which could not be detected at the time when the app was initially submitted for distribution.

(22) The EC has exacerbated the problem by forcing Apple to forego standards that it has applied since the launch of the iPhone. Developers can now use Apple's proprietary technology to distribute pornography, promote hate speech, and scam users.

(23) Apple has put in place risk mitigations. They are, however, far less effective than the previous system. Apple's users are now required to protect themselves, irrespective of their age or sophistication level, without any expectation of ever having to do so. End user interests are referenced (albeit inconsistently) by some DMA provisions but not by others. Children and elderly grandparents alike are now presumed to be on the lookout for scams, subscription traps, and other malicious schemes that Apple had previously been able to interdict.

(24) **User security and privacy should always be a valid basis to justify restrictions**. Some DMA provisions appear to prevent gatekeepers from taking any measures intended to protect end users. For example, Article 5(4) DMA requires Apple to allow developers to display in-app communications and promotions without recognizing any right for gatekeepers to impose limitations intended to protect users against malicious actors.[10] This is particularly problematic because the EC takes the expansive view that Apple must allow developers to send end users outside of their safe and familiar App Store environment into the open web without restrictions. This exposes users to an increased risk of fraud, scams, misleading pricing and invasion of privacy.[11] Web-based sales channels are not subject to the same rigorous checks as IAP purchases. They give bad actors the opportunity to engage in bait-and-switch tactics and evade parental controls. Link-outs amplify these risks by giving users the misleading impression that they are transacting with Apple or are otherwise under the umbrella of Apple's stringent security and privacy measures, which they are not in those circumstances.

(25) It would seem self-evident that user security and privacy should always be a valid basis to justify restrictions. Unfortunately, the EC's myopic approach to DMA enforcement ignores logic and focuses only on the commercial interests of a

---

10 *See, e.g.*, Center for European Policy Analysis, Reining in the Gatekeepers and Opening the Door to Security Risks, 2023 ("[*a*]*lthough these changes seem justified by conventional antitrust analysis, the DMA has been enacted without proper consideration of the danger of malign entities leveraging the regulation to wage economic or, even worse, military cyberwarfare*").

11 *See, e.g.*, Nokia Threat Intelligence Report, 2023 (attributing improvement in mobile infection rates to *"changes in app store security practices that ensure apps are screened for malware before they can be downloaded by users,"* highlighting the central role app store screening plays in reducing threats).

handful of large, successful developers. To ensure that logic and reason prevail, the DMA should explicitly acknowledge these principles across all obligations.

(26) **The EC's one-size-fits-all approach undermines customer choice.** The EC's misguided interpretation of the DMA requires providers of differentiated products to implement one-size-fits-all solutions, driving gatekeepers towards uniformity at the lowest common denominator. The EC's approach compels Apple to lower its privacy and security standards and degrade the seamless experience Apple users in Europe have come to expect.[12] What was meant to expand user choice ends up restricting it, limiting the ability to choose truly secure and private options. That cannot be the goal of the DMA but yet that is the consequence of the EC's radical interpretation of the DMA.

(27) The EC's approach requires Apple to redesign iOS to function more like Android. Time and again Apple has faced the EC making a direct comparison as to how a particular function works on Android. For example, the EC's specification decision in relation to connected devices expressly refers Apple to Android for inspiration. But the two platforms were built with two intentionally different philosophies. iOS was designed as a vertically integrated platform prioritizing user privacy, security, and seamless experience. Android was designed to operate on a broad range of devices of other OEMs, which inevitably comes to some extent at the expense of end user protections and ease of use. End users can freely choose between these distinct value propositions, based on their individual preferences. By compelling iOS to adopt Android's characteristics, the EC's enforcement undermines market differentiation, effectively reducing meaningful consumer choice.

(28) **The DMA has compromised access to innovative technologies for European consumers.** The EC's enforcement approach strips European consumers of the benefits of innovation.

(29) *Europeans no longer have access to innovative functionalities available in the rest of the world.* Apple has had to delay the release of several innovative products and features in the EU: Apple Intelligence reached the EU consumers after several months of delay; iPhone Mirroring and SharePlay Screen Sharing are still unavailable; and, this year, Apple had to withhold Live Translation via AirPods, the Visited Place functionality, and the ability to display iPhone's Live Activities to MacBook. This is not by choice. The extreme interpretations of Article 6(7) embraced by the EC have forced this outcome.

(30) The EC has interpreted Article 6(7), as it applies to Apple and Apple alone, to require complete parity of access for third parties to functionalities of iOS. In the EU,

---

12 In fact, several government agencies in the EU have reached out to Apple proactively to gain assurances that they could prevent their employees from taking advantage of the DMA's changes, in particular sideloading. *See, e.g.*, Reuters, Number of agencies have concerns about 'sideloading' on iPhone, Apple says, 2024.

this must happen at the same time as when Apple launches the new functionality. This approach fundamentally fails to recognize that enabling interoperability is not as simple as flipping a switch. Users have learned to expect that before Apple makes a sensitive functionality available to third-party developers—who can accidentally or deliberately misuse it—Apple will design the necessary safeguards. This takes time in some cases. In those cases where Apple cannot make third-party access available from the outset, the EC has told us we cannot release these functionalities in the EU.

(31) Apple has a well-earned reputation as an innovator with exacting standards for quality. Apple wants a high degree of confidence that the technologies and features it develops will work as intended when released to its hundreds of millions of users around the world. The challenge grows exponentially when Apple seeks to make some of these technologies and features available to the developer community. Apple wants to ensure that it fully understands how a technology or feature could be used—or misused—before opening it to third parties. The EC's radical interpretation of the DMA requires Apple to rush its development process and expose European users to new risks and threats.

(32) *The DMA deprives innovators of their intellectual property rights.* The EC's enforcement of the DMA has consistently disregarded Apple's intellectual property rights. Apple is one of the world's leading innovative companies. At the heart of our innovation lies ideas and experiences that only Apple can create through investment in research and development. Apple, like many others, protects those ideas with intellectual property. The law, until now, has allowed Apple to decide when, and if, it shares those ideas with third parties.

(33) The EC's specification decision in relation to connected devices imposed far-reaching obligations on Apple to provide third-party developers—including Apple's direct competitors, some of which are gatekeepers themselves—with access to Apple's proprietary, differentiating technologies in the EU, and to do so free of charge. Naturally, this interference with intellectual property rights undermines incentives to innovate—not just in the EU and not just for Apple.[13]

(34) Our users in Europe confront a new world crafted by the EC. The EC has decided that they are willing to delay Europeans' access to new products, technologies and features from Apple. The EC has decided this is a reasonable sacrifice in an effort to appease a handful of developers that want more access to European users' data and information. This is not a choice that Apple has made. Apple has consistently asked the EC to bring new technologies to Europe but give it time to open access to the developer community. The EC has refused. Apple has every interest to opening

---

13 The negative effects on incentives to innovate brought on by compulsory access are well described and documented in legal literature. *See, e.g.*, Robert O'Donoghue and Jorge Padilla, *The Law and Economics of Article 102 TFEU* (2020), pp. 609 et subs.

access to third parties. It has done so time and time again. However, Apple will not sacrifice access for safety, security, privacy and quality. The EC's approach to DMA enforcement has upended this delicate balance by ignoring the interests of users.

II. The DMA has failed to provide a fair regulation of digital platforms

(35) The EC has used the DMA to exclusively target American companies, deliberately allowing other large ecosystems to escape regulation and distort the playing field. This distortion is exacerbated by discriminatory enforcement of the law—heavily biased against Apple and, ultimately, its end users—due to the lack of procedural safeguards and the politicization of the EC's priorities. The EC has ignored the text of the DMA in favor of an ever-shifting articulation of the "spirit" of the law. Apple has little recourse other than to comply with their demands. The EC has demonstrated it is willing to use massive, arbitrary fines to force compliance with their interpretation of the law's spirit.

(36) From inception, Apple has adopted an integrated approach to its products: it designs hardware, operating systems, and software to function seamlessly together, ensuring a great user experience out of the box. This is what Apple's customers have come to expect from us. Other device manufacturers—including Samsung, the European market share leader—take a different approach, relying on third parties for their devices' operating systems. For example, Samsung has created an ecosystem of software and peripheral hardware that integrate with its smartphones. Yet Samsung is not subject to regulation. This one-sided regulatory approach is unfair and unjust. It allows other companies to compete freely in emerging spaces like augmented and virtual reality headsets and AI, without the shackles of regulatory constraints.

(37) Apple's user-centric privacy-focused business model is strongly aligned with core European values. Apple is still principally a hardware company, does not monetize user data, and cares deeply about the protection of minors. Despite this, no other gatekeeper had to make the same type of fundamental changes to its business model to comply with the DMA, and 5 out of 8 DMA investigations initiated so far concerned Apple.

(38) The record clearly shows that the EC's approach to its first two years of DMA enforcement has been neither objective nor impartial. It has instead pursued Apple, and only Apple, with demands for fundamental changes to our iconic products with disregard for our fundamental rights based on ideological outcomes that have no basis in the law.

(39) The EC has already (i) concluded two rushed and deeply flawed specification procedures in relation to interoperability under Article 6(7), (ii) concluded a steering investigation under Article 5(4), (iii) closed an investigation in relation to defaults and uninstallation, following Apple's implementation of EC demands, and (iv)

continues to run an investigation in relation to Apple's new business terms. Apple has received the highest fine so far under the DMA. Meanwhile, other companies have either completely escaped scrutiny, or investigations against them are inexplicably delayed far beyond those against Apple, despite being launched on the same day.

III. Specific provisions of the DMA should be amended to avoid clear harm

(34) The most effective way to repair the damage and prevent further harm would be a repeal of the law (or specific provisions) and a reset on digital competitiveness that puts users first. Absent that, we set out below a non-exhaustive list of changes to the DMA and the EC's current approach to its enforcement that could address ambiguity in the text, discriminatory enforcement, and procedural shortcomings that have exacerbated its negative impact.

A. Article 6(7) DMA

(35) Apple's deep integration between Apple's products and services is a critical part of what makes Apple's offering unique. Apple develops its hardware, operating systems, and related services with this integrated experience in mind. When Apple services and hardware interoperate, Apple is able to ensure that the necessary privacy, security and integrity protections for users are in place on its own devices and services.

(36) Apple has a long history of making its technology available to third parties free of charge for the benefit of the entire platform, including both users and developers. When deciding what technology to make available to third parties and when, Apple prioritizes technologies that will bring the most value to the most number of users, taking into account the possibility and technical complexity of doing so in a way that protects user security and privacy. This in turn benefits the widest swath of developers, by allowing them to serve the most users, and by allowing users to trust that developers are not going to misuse the core functionalities of their devices. The EC ignores this approach. Instead, the EC has interpreted Article 6(7) to require Apple to prioritize the interests of a few developers without balancing the interests of users who prefer having the highest level of security and privacy protections on their devices or other developers who may suffer from resources being diverted away from technology investments that would create broader benefits.

(37) Article 6(7) is fundamentally flawed in creating an unequivocal right for third parties to access Apple's technologies and failing to consider broader interests that should be taken into account. Those broader interests, and in particular interference with intellectual property rights, must be subject to proportionality, which is completely absent from the text. The EC has made no attempt to introduce proportionality in the enforcement of this provision, and the protection of such critical interests as user security and privacy and Apple's intellectual property rights should not be left

to interpretation. Even if it were possible to proportionately enforce the existing obligation that Apple provide access to its technology, the requirement that Apple does so free of charge is unlawful and at odds with the principles of innovation and contestability that the DMA purports to support.

(38) Article 6(7) should be repealed. Its failure to account for broader interests when putting Apple's technology in the hands of a few third parties is dangerous. Any obligation that would require Apple to provide its technology as a means of fulfilling regulatory objectives must be carefully circumscribed and should reflect an understanding of the technology at issue. There cannot be a one-size-fits all approach. Article 6(7) fails on all accounts and cannot be rectified short of a rewrite.

B. Article 5(4) DMA

(39) The App Store creates incredible opportunities for developers. It connects developers with billions of potential customers across the globe, who discover and download new apps from developers big and small because they trust the App Store environment. It is a place where customers make purchases with confidence because they trust Apple to protect them. And it offers many other benefits to developers, which Apple provides to them on an ongoing basis. Year after year, Apple invests heavily to make sure the App Store continues to provide developers and end users with that experience. This is only possible because Apple is fairly remunerated.

(40) The EC's extreme interpretation of Article 5(4) DMA denies Apple the right to fair remuneration. It enables developers to use all the tools, technologies and services which the App Store provides, while using the app as a billboard for directing customers to make their purchases elsewhere—evading any fees to Apple. This is fundamentally unfair and defeats Apple's incentives to continue to innovate for the benefit of all users.

(41) The most effective way to address these problems is a repeal of Article 5(4). The DMA's alternative distribution mandate is already fully effective in ensuring App Store contestability. End users and developers now have a choice between the App Store and a number of competing marketplaces on iOS and iPadOS—in addition to being able to move from Apple's platform to Android. The App Store is subject to fierce competition across the board. Apple therefore must be allowed to run its own store in the way that it considers best to compete. The way in which Apple seeks compensation for its App Store services is controlled by market forces. This leaves no room for regulatory interference.

(42) Short of repeal, the text of Article 5(4) should be explicitly narrowed to its originally intended purpose: a simple and straightforward obligation to allow developers to *inform* their users that they can buy the developer's content and subscriptions on its webpage. By contrast, Article 5(4) was never intended to regulate the fees which

Apple can charge where it facilitates transactions. Yet, the EC has forced this interpretation which Apple must follow pending appeal. It should be made explicit in the text that this was not the intention of the law. The language should be amended to explicitly allow a gatekeeper to charge for services rendered to developers.

(43) At a minimum, the text should be amended to take into account consumer interests such as safety, privacy and security. The threat from fraud, scams, subscription traps and misleading or deceptive behavior is increasing year after year. It makes little sense to expose users to these risks and hope that they are sophisticated enough to detect the threat.

C. Article 6(4) DMA

(44) Article 6(4) was intended to promote contestability of gatekeepers' own app marketplaces. While the alternative distribution mandate inevitably reduces Apple's ability to protect its end users, its purpose can be achieved without wholly upending Apple's platform built on users' trust. Allowing robust, capable and responsible third-party app marketplaces to distribute on iOS and iPadOS would be fully effective to challenge gatekeepers' marketplaces. By contrast, web distribution is far less likely to have any effect on gatekeepers' incentives with regard to how they operate their marketplaces but introduces a huge host of risks that Apple cannot protect its users against.[14] Yet, the EC has unnecessarily interpreted Article 6(4) DMA as requiring gatekeepers to allow *all forms* of alternative distribution, including web distribution. The EC's overly broad interpretation degrades, rather than promotes, competition by depriving users of their ability to choose an Apple device knowing that they will benefit from the highest level of protections.

(45) Article 6(4) DMA should be amended to make it even clearer that gatekeepers are only required to allow one form of alternative distribution provided it is effective, which is the case for alternative app marketplaces. This would provide users with access to apps outside of the App Store and allow developers the ability to distribute their apps according to other distribution models not controlled by Apple, in full compliance with the existing objective. Other gatekeepers would remain free to enable web distribution if they chose to differentiate their platforms by maximizing distribution options, accepting a riskier environment for users.

D. Article 6(3) DMA

(46) Article 6(3) DMA should be repealed. It was designed to ensure that choice was presented to users. So far, the most tangible outcome of Article 6(3) of the DMA

---

14 *See, e.g.*, Chamber of Progress, New Campaign: How Digital Markets Act Has Become Europe's Digital Curtain, 2025 (*"[t]he forced modularity mandated by the DMA has created security gaps and exposed users to greater fraud and cybersecurity threats. The introduction of third-party app stores and sideloading has created new vectors for malware and bad actors, potentially compromising user data"*).

has been the imposition of an anti-Safari browser choice screen on iOS and iPadOS. Apple has long made it easy for users to choose a browser as a default going back to iOS 14. Instead of empowering users, the choice screen interrupts the user experience that Apple has carefully crafted by assuming users do not understand their choices. It burdens all EU users with unnecessary friction for the sake of a theoretical concern that does not reflect actual user demand.

(47) The other Article 6(3) obligations are equally ineffective and disproportionate. For example, the scope of the uninstallation requirement has proven problematic. After complying with the EC's requirements, all apps but Phone and Settings can be removed from iOS and iPadOS. In an attempt to address a purported concern—the substance of which is unclear, particularly given that apps were already removable from the Home Screen—this obligation represents a further deterioration of the user experience. It introduces unnecessary complexity and confusion, which could result in EU users accidentally deleting apps or being unable to recover them.

IV. Additional changes would help mitigate the negative impact of the DMA

(48) The DMA does not account for different business models, different competitive dynamics, and different risks associated with all the digital services of separate providers that are swept into its obligations. It has been applied in ignorance of these distinctions—or worse, with a view towards eliminating these differences and reducing the market to the lowest common denominator. Short of the immediate repeal of the law or specific provisions, some changes could be made to address the ambiguity in the text, biased enforcement, and procedural shortcomings that have exacerbated its negative impact.

A. Ambiguities in the text of the DMA should be clarified

1. The DMA should explicitly incorporate proportionality to protect end user interests

(49) In its DMA enforcement to date, the EC has consistently prioritized the interests of a few large developers over end users. In every instance, the EC has insisted on the broadest possible interpretation of an obligation that could benefit certain developers, and refused to accept consideration of end users' interests. This has come at a cost to the safety, security, privacy, and overall experience of EU end

users and the innovations available to them, and unjustifiably interferes with Apple's IP rights.[15]

(50) The DMA does not clearly and consistently describe by reference to which countervailing (end user) interests proportionality should be assessed. Integrity, security, and privacy are referred to as some justifiable grounds for protective measures inconsistently across provisions, and in many cases not at all. This has led to protective measures being arbitrarily possible for some values in some contexts but not others, which makes no sense. Values such as these are not context-dependent and should be protectable across the board.

(51) There should be an explicit overarching proportionality test applicable to all provisions to ensure the DMA objectives can be achieved without unjustified harm to widely recognized interests of end users. Relevant factors reflecting user interests should be explicitly identified, including the safety, security, privacy, device integrity, overall experience of users, promotion of user choice (not only intra-platform, but also inter-platform), and access to innovation, and these factors should be subject to a balancing exercise in each case.

(52) An overarching proportionality test should also explicitly consider the rights of gatekeepers, such as intellectual property rights and the right to conduct their businesses, including through product differentiation. Individual provisions should also incorporate specific proportionality factors into their respective obligations. For example, Article 6(7) should take into account the extent of interference with property rights and the freedom to conduct a business. This test should also make plain that requirements like Article 6(7) do not mandate the creation of functionalities for which there is no material market demand. This would ensure the contestability aim served by providing interoperability justifies the resources required to do so, which could otherwise have been invested in developing other technologies to the benefit of business users and end users. By explicitly introducing proportionality in these ways, compliance with the DMA could be effective without needlessly destroying the benefits that Apple's platforms have generated for users in the EU.

---

15 *See, e.g.*, Centre for Data and Innovation, European Consumers Are Right to Complain About the DMA, 2025 (*"European consumers report a worse online experience since the Digital Markets Act (DMA) took effect, according to a recent survey of 5,000 people by Nextrade Group, a firm specialising in digital trade research. This perception is not just subjective—the DMA required companies to make functional changes to their digital products and services in ways that directly align with consumer complaints. The findings underscore how, when regulators rather than the private sector dictate technology design, consumers ultimately lose out".* […] *The evidence is clear: The DMA has not improved consumer outcomes and has instead made many users worse off by forcing unwelcome changes on the digital products and services they rely on"*).

2. "Effective compliance" should focus on the text of the law

(53) The EC relies heavily on the notion of "effective compliance" to embrace sweeping interpretations of obligations that are untethered by the text of the law. The EC's interpretation of "effective compliance" is misaligned with Article 8(1). The EC has substituted achievement of the objectives with achievement of actual market outcomes. This interpretation of "effective compliance" is at odds with the foundation of the DMA, which is designed to create fair opportunities for end users and business users.

(54) The EC's aggressive efforts to redistribute value to developers or shift market share to competitors is without legal basis and distorts the incentives for business users to innovate. Against this outcomes-based standard, the loudest third parties have simply characterised compliance as whatever outcome maximises their own interests. This pandering to the whims of those who shout the loudest is exacerbated by the EC's reliance on awaiting the outcome of market tests before forming a view on how the DMA should be interpreted. Market tests are targeted inevitably by those who are the most incentivized to seek to maximize their own commercial interests.

(55) When prejudged results are the starting point, it is impossible to weigh the interests of all relevant stakeholders properly to ensure a proportionate interpretation of an obligation. Compliance cannot be about outcomes for individual third parties, but fulfilling the obligations related to specific conduct. Constructive regulatory dialogue should likewise focus on how Apple carries out compliance, rather than whether specific market results are achieved to the satisfaction of Apple's competitors. This should be made clearer in the DMA to prevent the EC weaponizing its discretion as enforcer of the DMA to mandate specific outcomes, which undermine competition and innovation and the fruits of them for EU users and businesses.

B. The DMA should be enforced predictably, equitably, and in the interest of innovation

(56) A company has the right to know what the law is in order to comply with it. The EC must be required to clearly articulate its interpretation of the law prior to opening an investigation into non-compliance with that law. The EC should not impose fines for conduct deemed non-compliant that took place at a time when the EC's own view of compliance was still evolving.

(57) The EC has disregarded these basic principles of predictability and legal certainty in its DMA enforcement. The EC's legal interpretations have continuously shifted over time. Apple was faced with a shifting definition of compliance by the EC regarding alternative distribution, interoperability, choice screens and other topics. Article 5(4) DMA stands out. The EC has applied different standards to different companies. In its rush to impose a blockbuster fine, it ignored procedural safeguards and

fundamental principles of fairness. Rather than articulating a clear view of compliance from the outset, the EC kept Apple guessing throughout the informal engagement period and throughout the investigation. Each time Apple proposed a solution that met the EC's principles, the Commission moved the goalposts. Nevertheless, this enormous uncertainty did not stop the EC from imposing a blockbuster fine for non-compliance—including for the entire period pre-dating the decision, when Apple was actively working with the regulator to achieve compliance and pleading for guidance on the same.

(58) Enforcement should actively avoid creating benefits for gatekeepers. For example, gatekeepers that have their own platform technology to provide their services should not be permitted to submit interoperability requests. There is already clear recognition in EU law of the need to ensure that gatekeepers cannot seek to weaponize laws designed to apply to them in ways that will effectively unwind and undermine obligations applied in another area of the law.

(59) The EC should be mindful that overzealous enforcement can stifle innovation.[16] For example, Apple's AI technology is still in the nascent phase of development. Any concerns involving Apple's core platform services and AI technology are purely speculative at this point. Early consideration of enforcement in this space would distract Apple from critical innovation efforts, deter development and ultimately impede the launch of high quality AI products for end users in the EU. Careful and transparent setting of enforcement priorities would help avoid those risks.

C. Enforcement by an Objective Agency

(60) Apple's experience with the DMA enforcement shows that the EC has been highly responsive to external pressures—whether from complainants or from shifting political enforcement agendas—resulting in a disproportionate focus on Apple. But the DMA should be a technical instrument, applied by technical experts in a manner that is strictly aligned with the legislative text, proportionate, and respects fundamental rights. Instead the EC has treated the DMA as a weapon, adopting a persistently adversarial stance uniquely against Apple that is wholly inappropriate for this regulatory framework. The only credible solution is to entrust DMA enforcement to an independent European agency, shielded from political interference and able to ensure fair, balanced, and text-based application of the DMA.

---

16 *See, e.g.*, Christian Năsulea and Diana Năsulea, Rethinking the DMA: Innovation, Competition, and the Risks of Overregulation, 2025 ("*[m]ajor tech companies have postponed or limited the introduction of new features due to regulatory uncertainties, resulting in European consumers and businesses receiving access to these advancements later than their global counterparts*").

D. Coordination with Subject-Matter Regulators and Agencies

(61) The EC should place far greater reliance on the relevant subject-matter regulators and agencies.[17] The DMA implicates many other policy areas involving how tech companies operate, such as data protection and cybersecurity. Enforcement of the DMA in a way that achieves its objectives without undermining broader EU policy goals requires a great deal of coordination and technical expertise. The DMA explicitly recognizes this complexity in establishing the high-level group pursuant to Article 40. At any moment, the EC can request meetings of the high-level group to draw on their superior expertise. Surprisingly, the full group has met only 5 times, largely to discuss the formation and reporting of sub-groups, and there have otherwise only been 9 meetings of the three subgroups formed to discuss discrete issues related to Article 5(2), Article 7(2), and AI. Notably, the obligations in relation to which Apple has been subject to proceedings—Articles 5(4), 6(3), 6(4), and 6(7)—have not triggered a single discussion within the high-level group despite the many arguments Apple has made about privacy, security, and consumer welfare. This suggests that the EC is minimizing expert input on potential clashes between its enforcement actions and other protected interests and values. Apple has seen no evidence of the involvement of the High-Level Group in any of its engagements with the EC.

(62) For example, providing interoperability solutions to third-party developers under Article 6(7) is highly technical, involving privacy, security and intellectual property considerations. Given the broad obligation to provide "effective interoperability" and the existence of multiple possible solutions for doing so, the EC should take informed action in coordination with other agencies to ensure compliance is achieved in a way that best serves the DMA without unnecessarily interfering with other policy objectives. Input from other agencies, like the European Union Agency for Cybersecurity, would provide a valuable steer on which solution among all those that could provide effective interoperability would be a better choice to achieve compliance with the DMA while protecting the privacy and security of users and respecting fundamental rights.

(63) DMA obligations related to access and use of data should be enforced in a way that is consistent with broader data rules and supports coherent data practices. The EC's enforcement priorities should furthermore consider the impact on Apple's ability to maintain its industry-leading privacy protections that have been applauded by other agencies like national data protection authorities. Those agencies should

---

17 *See, e.g.*, Belle Beems, The DMA in the broader regulatory landscape of the EU: an institutional perspective, European Competition Journal, 2023 (arguing that a forum of cooperation between competition law, consumer law, data protection law and the DMA "*can be very important for the effectiveness of the DMA, but also gives broader insights on the position of the EU legislator vis-a-vis Big Tech and reflects the need to look beyond the traditional boundaries between legal branches*").

be meaningfully involved, as a matter of course, whenever data protection is at stake.

E. Procedural changes

1. The numerical approach to designation adopted by Article 3 DMA is flawed

(64) The DMA's rigid reliance on quantitative thresholds to designate gatekeepers fails to account for an undertaking's actual significance as an intermediator between business users and end users. Absolute size is no proxy for market influence and user dependency, which can only be assessed through an overall evaluation of qualitative factors such as an undertaking's position relative to that of competitors, data advantages, network effects, multi-homing and switching.

(65) The rationale for selecting the specific thresholds as the benchmark for gatekeeper power remains shrouded in obscurity. The DMA Impact Assessment observes that higher thresholds would result in the designation of 5–7 gatekeepers, whereas lower thresholds would result in 10–15. This suggests that the legislator backwards-engineered the criteria to allow for the desired outcome. Two years on, the outcome is clear: the DMA's quantitative threshold resulted in the designation of 7 gatekeepers, only one of which is EU-based and 5 of which are US-based.

2. Designation rebuttals

(66) If the legislator decides to maintain the DMA's flawed quantitative presumption, there should at a minimum be a meaningful opportunity for presumptive gatekeepers to rebut the presumption by advancing qualitative criteria in respect of their core platform services. This does not correspond to the EC's current interpretation of the DMA, which results in a distorted evidential standard.

(67) First, Article 3(8) DMA includes a long list of qualitative criteria which the EC can take into account when *designating* a core platform service that does not meet the quantitative thresholds. But the EC refuses to take these same criteria into account when assessing *rebuttals* of a quantitative presumption. The EC takes the position that only those criteria which are closely related to quantitative criteria matter in that context. This is devoid of logic and manifestly unfair. It cannot be rationally explained why the same qualitative criteria for assessing a gatekeeper status should not apply in both scenarios.

(68) Second, the main quasi-quantitative criterion considered by the Commission for rebutting the presumption seems to be the demonstration of a very small market share (e.g., TikTok Ads, X Ads, Samsung Internet browser, Microsoft Advertising). Successful rebuttals in these cases have involved services with market shares of less than 5%. This makes little sense, considering the close relationship between the notion of dependency on an important gateway and a dominant position. Based

on the EU Courts' decisional practice, dominant positions often require market shares of 50% or more. There is no reason to assume that a service which meets the quantitative thresholds and has a market share of for example, 20% or 30% has the characteristics of a bottleneck between business and end users. Whether this is the case depends on a detailed overall assessment of all relevant qualitative criteria. However based on the Commission's practice, the presumption is almost irrebuttable in such circumstances, and many qualitative arguments are deemed simply inadmissible and will be disregarded, however compelling they may be in substance. This is yet another example of the EC unlawfully exploiting its discretion under the DMA to engineer its desired outcome.

3. The DMA should provide for a formal commitments procedure

(69) Once a non-compliance investigation is opened pursuant to Article 29, the Commission can only adopt a non-compliance decision or close the proceedings by a decision. The lack of a formal commitments procedure (comparable to Article 9 Regulation 1/2003) impedes the continuity of constructive regulatory dialogue and prevents efficient resolution. In practice, in some cases settlements have been informally reached, for example, in relation to the EC's investigation of Apple for alleged non-compliance with Article 6(3). But the lack of a formal commitments procedure in this context enables the EC to exploit the threat of fines to extract changes that go far beyond a reasonable interpretation of the law, without any certainty for the gatekeeper that the implementation of those changes will actually terminate the proceedings.

(70) To facilitate procedural efficiency and ensure fair outcomes, a structured commitment procedure should be established. This would facilitate open dialogue during infringement proceedings, where both sides have an interest in protecting their legal position while pursuing a compliance resolution in parallel. A formal framework should provide assurance to the gatekeeper that in exchange for accepting the commitments, the procedure will be closed without fines or finding of an infringement.

4. Reforms to the specification procedure

(71) A central flaw of the DMA is the ambiguous and high-level drafting of Articles 5–7, which generates a great deal of regulatory uncertainty for gatekeepers, end users, and business users. Article 8 purports to address this challenge by granting the Commission a broad discretion to specify how a gatekeeper must comply in any

given case. However, the very first, and only, experience with using that procedure —again, against Apple—has revealed important shortcomings.[18]

(72) First, the current rules disincentivize the Commission from running a specification investigation thoroughly and diligently, which would be consistent with the technical complexity of issues at hand. For example, very ambitiously, the Commission extended the scope of the specification procedure in relation to connected devices to around 15 discreet functionalities of iOS, each raising distinct technical and legal issues. Yet the Commission allocated only two months for its investigation before it rushed to issue preliminary findings proposing third-party access to some of the most sensitive iOS functionalities and user data. To mitigate this going forward, the DMA should be adjusted to:

- Require case-specific timelines proportionate to the scope of complexity of the specification, with a clear ability to extend if necessary;
- Provide for a staged or modular specification where multiple functionalities are at issue, allowing for deeper inquiry and stakeholder input;
- Mandate targeted consultation of independent technical experts and affected stakeholders.

(73) Second, Article 8 should be clarified to prevent the Commission from prescribing measures that go beyond substantive compliance. The specification procedure is intended to clarify existing obligations. The Commission should not use it to redraft the DMA by creating new duties or dictating internal procedures, such as forcing Apple to implement a burdensome and bureaucratic interoperability request process.

* * *

18 *See, e.g.*, Computer and Communications Industry Association Europe, New Study Finds DMA Procedural Flaws Hinder Compliance and Enforcement, Proposes Fixes Ahead of Review, 2025 (*"DMA procedural mechanisms remain opaque, overly complex, and heavily dependent on the Commission's broad discretion"* and *"current procedures, including informal dialogue, are hindered by tight timelines and legal uncertainty"* which *"creates challenges not only for gatekeepers, but also for third parties seeking access under the DMA".* The study also flags that *"[t]his lack of clarity and transparency […] creates significant practical difficulties for all parties, with knock-on effects for business users and consumers"*).