ECIPE | EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY

POLICY BRIEF – No. 04/2025

Cybersecurity at Risk: How the EU’s Digital Markets Act Could Undermine Security across Mobile Operating Systems

Matthias Bauer *and* **Dyuti Pandya,** *Director and Analyst at ECIPE*

EXECUTIVE SUMMARY

The EU's fight against cybersecurity threats risks being undermined by the over-enforcement of the Digital Markets Act (DMA). Article 5(4) could force mobile operating system providers to allow unregulated external links, bypassing critical security controls and exposing millions of smartphone users to cyber threats.

The 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.

The unintended consequences of this regulatory approach are already evident in Apple's recent decisions to withhold certain features – such as advanced AI functionalities and enhanced app security tools – from the EU market due to DMA-related concerns. As a result, EU consumers face reduced access to innovative technologies, diminished user experiences, and weaker security protections compared to users in other regions. Now, Android, a widely used open-source system, may also be compromised by DMA enforcement, potentially limiting its flexibility, security, and the broader ecosystem of app developers and device manufacturers that rely on its open architecture.

To balance competition and security, EU policymakers should:

1) **Ensure Technology Neutrality:** The DMA should remain technology- and architecture-neutral, allowing competition between ecosystem models that prioritise security and trust.

2) **Uphold Regulatory Coherence:** Align the DM A with the EU's broader cybersecurity framework to prevent conflicts with regulations like NIS2 and the Cyber Resilience Act.

3) **Recognise Platform Differences:** Tailor competition policies to different operating systems, as a one-size-fits-all approach risks weakening consumer protection.

4) **Preserve Security Measures:** Allow OS providers to block unvetted third-party linkouts to prevent malware and fraud, with mandatory verification for external links if required.

5) **Exempt Justified Security Actions:** Exempt providers from DMA penalties when restrictions are necessary to address imminent, evidence-based cybersecurity threats.

1. THE DIGITAL MARKETS ACT (DMA) AND ITS POTENTIAL CYBERSECURITY RISKS

Sometimes the extreme example helps to illustrate a point. As the Digital Markets Act (DMA)[1] was going through the motions in Brussels and European capitals, some observers (like these authors) called for guidance from and disciplines of the regulator to create greater clarity and predictability about what different DMA provisions actually would entail for certain Core Platform Services hosted by gatekeepers.[2] At the time, the prevailing attitude was muscularly suspicious of any such attempts, treating such calls and – following principles of good regulation – a general need for feedback loops about the results of the DMA as submissions to the power of Big Tech.[3]

It was sometimes acknowledged that the DMA could have adverse regulatory effects, in the worst-case causing firms to having to violate one regulatory provision or objective in order to comply with another provision or objective. Data security and, more generally, cybersecurity was one such area – objectives acknowledged in the DMA but packaged into an overall structure of regulation that it did not create clear interpretations about what is most important: forcing choice and openness on platforms or preserving cybersecurity and a general trust architecture? Such questions were unanswered, and we are now witnessing the consequences. The question remains: How can we avoid that the DMA compromises data security and generally prompts a deterioration in user security for those using various platform services?

The extreme example concerns Apple and EU DMA demands to prioritise platform openness rather than user security. A third-party platform has now been able to offer in Apple's App Store a pornographic app that Apple does not want to include in its ecosystem.[4] This particular app is now branded as "Apple approved" for the simple reason that Apple is forced by the DMA to allow access to it in the EU, and the US company reasonably makes the argument that it would like to reject access to it because it violates the trust architecture that is key for the company and its users. While the DMA takes a narrow view of security-related issues, focusing mostly on technical aspects, the reality is that Apple and its main competitors have built up a trust architecture over a long period that can come to sit awkwardly with the DMA principle to give priority to forcing openness and choice on mobile platforms.[5]

A principal friction between security and openness have also emerged in other EU but non-DMA cases. While reasonable antitrust concerns have been raised against limited access and high access fees for using certain Apple services – for instance, NFC-based mobile payment apps – there have also been unreasonable demands and proposals on openness that compromise security, which were forced on Apple. And there is an urgent need for regulatory clarity.

[1] EU Digital Market Act. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R1925.

[2] European Commission (2025). Gatekeepers. Available at https://digital-markets-act.ec.europa.eu/gatekeepers_en.

[3] ECIPE (2022). The EU Digital Markets Act: Assessing the Quality of Regulation. Available at https://ecipe.org/publications/the-eu-digital-markets-act/.

[4] See, e.g., Bloomberg (2025). Available at https://www.bloomberg.com/news/articles/2025-02-03/apple-blasts-eu-app-laws-after-first-porn-app-comes-to-iphones?utm_source=website&utm_medium=share&utm_campaign=copy.

[5] Barczentewicz, M. (2023). Interpreting the EU Digital Markets Act Consistently With the EU Charter's Rights to Privacy and Protection of Personal Data. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4531383.

The EU has made cybersecurity a cornerstone of its digital sovereignty and economic security agenda. Initiatives like the EU Cybersecurity Strategy, the Cyber Resilience Act, and the Network and Information Systems (NIS2) Directive highlight the EU's strong commitment to protecting its digital landscape and strengthening cyber defences.[6] Billions of euros have been and will be invested by EU entities to safeguard critical infrastructure, enhance cyber resilience, and protect consumers from online threats. The European Commission's enforcement of the DMA may risk significantly undermining these very efforts.

A new instance of the conflict between openness and security has emerged, and it is important to understand it better, especially considering that platform providers operate under different business and technology models. One of the most contentious aspects of the DMA is Article 5(4), and hits is now used to require Google to allow developers to insert links inside their Play Store apps, leading users to external offers such as alternative payment methods, special in-game promotions, or other third-party content.[7] Google's compliance proposal, known as the External Offers Program (EOP), aims to balance regulatory obligations with cybersecurity protections.[8]

This regulatory tension is not unique to one app ecosystem. As already noted, Apple, for instance, has faced similar scrutiny regarding NFC access and App Store payment systems, with regulatory demands undermining its tightly controlled security framework. In fact, recent DMA-related cases have already led Apple to withhold certain functionalities, such as new AI features in iPhone 16, from the EU market due to security concerns tied to regulatory uncertainty.[9]

The European Commission is currently investigating whether Google's EOP fully complies with the DMA. One of the primary concerns raised by regulators is Google's security policy, which prevents developers from linking directly to third-party apps or alternative app stores from within Google Play's trusted environment.[10]

Google restricts unverified third-party links in Play Store apps such as those leading to phishing pages or malware to protect users from cyber risks. Mandating unrestricted linkouts would dismantle key security protections, exposing millions of EU users vulnerable to malicious software, fraudulent scams, and covert data gathering.

[6] See, e.g., European Commission (2024). Cybersecurity Policies. Available at https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies#:~:text=The%20Digital%20Europe%20Programme%2C%20for,public%20administrations%2C%20businesses%20and%20individuals.

[7] Oppenhoff (2024). EU-Commission opens first DMA investigations against Apple, Meta and Alphabet. Available at https://www.oppenhoff.eu/en/news/detail/eu-commission-opens-first-dma-investigations-against-apple-meta-and-alphabet/.

[8] Google (2025). Enrolling in the external offers programme. Available at https://support.google.com/googleplay/android-developer/answer/14372887?hl=en-GB.

[9] European Commission (2024). Commission accepts commitments by Apple opening access to 'tap and go' technology on iPhones. Available at https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3706. Also see, e.g., The Guardian (2024). Apple delays launch of AI-powered features in Europe, blaming EU rules. Available at https://www.theguardian.com/technology/article/2024/jun/21/apple-ai-europe-regulation. Also see Apple (2024). Complying with the Digital Markets Act – Apple's Efforts to Protect User Security and Privacy in the European Union. Available at https://developer.apple.com/security/complying-with-the-dma.pdf.

[10] European Commission. (2024, March 25). Commission opens non-compliance investigations against Alphabet, Apple and Meta under the Digital Markets Act. Press Release. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1689.

1) **Bypassing Google Play Protect:** Play's security framework relies on continuous threat scanning. Allowing unvetted external links would create a major security gap, weakening existing safeguards, and enabling threat actors to distribute malicious APKs, hijack accounts via fake login pages, or deploy spyware undetected.[11]

2) **Increased Malware Exposure:** Cybercriminals could release an app that appears to be legitimate on Play, and then use external links to redirect users to malicious sideloaded apps that evade Google's vetting.[12]

3) **Sideloading – The Primary Source of Android Malware:** Over 95% of malicious Android apps originate from sideloading, not from the Play Store. Unverified app stores are key vectors for banking trojans (e.g. Anatsa, Xenomorph), spyware (e.g. Mandrake spyware, SMSVova), and counterfeit apps mimicking legitimate services to steal credentials.[13]

Unverified third-party linkouts from Google Play could thus substantially compromise user security, enabling scams, spyware, and privacy breaches. Malicious actors can deceive users – especially children – into downloading harmful apps that steal data, lock devices, or enable sextortion.

It is important to question the added value of forcing third-party linkouts in an ecosystem where sideloading is already possible. Android users who wish to install apps outside of Google Play can already do so, albeit with additional security steps. This friction is not an arbitrary obstacle but a necessary safeguard against malware, phishing, and spyware. By mandating third-party linkouts, the DMA does not enhance user choice – it merely weakens essential security barriers designed to protect consumers.

While Google Play's protection measures are robust, they are not foolproof, as malicious apps occasionally slip through or exploit linkouts to external sources. Stalkerware disguised as parental control apps is increasingly used for domestic surveillance, while spyware via linkouts can extract private messages, contacts, and even activate a user's camera or microphone.[14] These apps tend to bypass Google's policies by disguising true functionalities until post installation. Financial fraud risks through fake banking apps and overlay attacks (recording login details) also

[11] Google Play Protect (2024). Available at https://developers.google.com/android/play-protect.

[12] See, e.g., Usercentrics (2024). Top data privacy issues for apps, games and web publishers. Available at https://usercentrics.com/knowledge-hub/2024-privacy-challenges-for-apps-and-games-publishers/.

[13] See, e.g., Forbes (2024). Google Play Store Warning—95% Of 'Malicious Apps' Come From Sideloading. Available at https://www.forbes.com/sites/zakdoffman/2024/10/11/google-play-store-new-app-warning-for-samsung-galaxy-s24-pixel-9-pro-android/.

[14] See, e.g., Sky News (2024). 'I thought I'd been microchipped': How abusers spy on partners with 'parental control' apps. Available at https://news.sky.com/story/i-thought-id-been-microchipped-how-abusers-spy-on-partners-with-parental-control-apps-13272199?utm_source=chatgpt.com.

rise as attackers exploit these vulnerabilities to steal banking details and sensitive data,[15] all of which poses risks to financial security, personal privacy, and corporate data worldwide.[16]

Moreover, regulatory disparities create additional concerns. While the DMA imposes strict obligations on certain platforms, it does not cover major Chinese app ecosystems, which will continue to offer tightly interlinked services without equivalent security oversight. This regulatory gap not only provides an uneven playing field but also introduces new avenues for data exposure and potential exploitation. Ironically, such outcomes contradict the EU's broader strategic goal of reducing dependency on Chinese digital infrastructure and enhancing data sovereignty. By inadvertently privileging non-EU platforms that face fewer restrictions, the DMA risks undermining the very cybersecurity and geopolitical resilience objectives it seeks to promote.

The application of the DMA should be technology and architecture neutral, allowing for competition between different ecosystem models that all make big efforts to control security and increase trust in their platforms. Operating system providers are generally in the best position to vet and block such malicious apps, ensuring user safety. Commercial incentives compel them to conduct robust security checks, safeguarding user security and sustaining competitive advantage. While the EU seeks to lead in cybersecurity, it must ensure that competition enforcement does not come at the expense of user safety. This Policy Brief examines why Android's security model differs from iOS, highlighting the risks of a one-size-fits-all approach, the cyber threats posed by malicious sideloaded apps, and Google's security measures to protect users from fraud and malware. It also provides policy recommendations to balance competition enforcement with cybersecurity safeguards, ensuring that user safety remains a priority.

2. OPEN VS. CLOSED OPERATING SYSTEMS: UNDERSTANDING THE SECURITY RISKS

Ironically, the DMA's push for increased openness in mobile operating systems may have the opposite effect. By requiring Android to allow unrestricted third-party linkouts, the European Commission creates a security dilemma: remain open and face higher security risks or become more restrictive like Apple's closed ecosystem. If Android were to shift towards iOS-style security policies, it would reduce device customisation, likely increase prices, and limit competition by reducing market diversity. Rather than fostering competition, the DMA's rigid approach risks strengthening the dominance of existing players while raising barriers for new entrants.

Rules like the DMA focus primarily on market structure rather than the technical structure of operating systems, overlooking how variations in system design directly impact security vulnerabilities. This narrow focus risks creating regulatory blind spots, as it fails to consider how different technical architectures – such as open versus closed ecosystems – require distinct security approaches. Imposing one-size-fits-all rules, like mandating third-party linkouts under uniform conditions, ignores these critical differences. Such an approach could undermine user

[15] See, e.g., Data Economy (2025). Google just made it harder for scammers to trick you: Here's how. Available at https://dataconomy.com/2025/01/30/google-just-made-it-harder-for-scammers-to-trick-you-here-is-how/.

[16] See, e.g., Verimatrix (2024). 100 Mobile App Threats to Watch in 2024. Available at https://www.verimatrix.com/cybersecurity/cybersecurity-insights/100-mobile-app-threats-to-watch/.

safety by weakening platform-specific security safeguards, particularly in more open systems where the risk of harmful app proliferation is higher. To ensure both robust competition and strong cybersecurity, regulation must be nuanced, accounting for the unique technical and security models of each platform.

While both Android and iOS allow external links, their security architectures differ significantly. Apple operates a closed ecosystem, reviewing and notarising every app before installation, thereby minimising security risks. In contrast, Android's open model provides greater flexibility but also demands stronger security measures to protect users from cyber threats (see Table 1).[17] Importantly, Android is different from iOS in its fundamental approach to app distribution and security. Apple's App Store hosts about 2 million apps,[18] all subject to strict review before release – every app must go through a stringent review and notarization process before being made available on the App Store. This tightly controlled environment limits the risk of unvetted software but also restricts user flexibility.

In contrast, Google's Play Store operates within a more open framework, offering close to 4 million apps and allowing third-party installations. Chinese manufacturers also run Android-based app stores, led by Huawei AppGallery with 44% of the market, alongside Tencent, Xiaomi, Baidu, OPPO, and others.[19] While this enhances user choice and innovation, it also introduces security risks, as apps downloaded outside the Play Store may bypass Google's security checks, increasing exposure to malware, fraud, and data breaches.

To safeguard its users, Google Play already employs a comprehensive multi-layered security framework, including Google Play Protect, rigorous app vetting, and continuous security monitoring (see Section 3 below). However, overenforcement of Article 5(4) of the DMA would jeopardise user safety by forcing Google to allow unvetted third-party linkouts within Play Store apps. If irresponsibly enforced, the DMA could create a major cybersecurity loophole, along with DMA's data sharing requirements may enable foreign rivals (including adversarial states) to access sensitive data or trade secrets,[20] making the EU a prime target for cybercriminals.

[17] See, e.g. Garg and Baliyan (2024). Comparative analysis of Android and iOS from security viewpoint. Available at https://www.sciencedirect.com/science/article/abs/pii/S1574013721000125.

[18] Caminade, J. and Wartburg, V. M. (2022). The Success of Third-Party Apps on the App Store. Analysis Group. Available at: https://www.apple.com/newsroom/pdfs/the-success-of-third-party-apps-on-the-app-store.pdf

[19] See, e.g., Bankmycell (2025). How Many Apps In Google Play Store? (2025). Available at https://www.bankmycell.com/blog/number-of-google-play-store-apps/#:~:text=How%20Many%20Apps%20on%20Google%20Play%20(2009%2D2025).

[20] Suominen, K. (2024, March 22). New Costs and Cybersecurity Challenges Flagged as DMA Compliance Starts. CSIS. Available at: https://www.csis.org/analysis/new-costs-and-cybersecurity-challenges-flagged-dma-compliance-starts

TABLE 1: COMPARISON OF IOS[21] AND ANDROID[22] SECURITY MODELS

Aspect	iOS (Closed System)	Android (Open System)
App Review Process	Strictly reviewed and notarised **before installation, minimising risks,** conducted according to a basic set of rules outlined in the App Store Review Guidelines. Developers must be registered	Both automated reviews and human reviews. Apps undergo security checks, **but users can install apps from outside Google Play.** Anonymous developers allowed.
External Links	Permitted **under strict oversight;** Apple retains control over security. Limited to Safari-based web experiences.	Allows **greater flexibility,** but **unvetted external links increase risks.**
Code Integrity	Mandatory code signing – only Apple signed apps run on non-jailbroken devices.	Google Play apps are signed, but third-party APKs can bypass this, malware can exploit sideloaded apps (FluBot via fake APKs).
Malware Risk	Lower risk **due to Apple's controlled environment.**	Higher risk **due to sideloading;** 95% of malicious apps originate from outside Play Store.
Security Protections	App installations are tightly controlled to prevent malware infiltration.	Google Play Protect scans apps for malware and monitors them after installation.
Update Frequency	Rapid, unified updates: majority of iOS devices run the latest OS within 2 months. Critical security patches deployed within days.	Fragmented, fewer Android devices run Android 13+ – security patches happens monthly, bi-monthly or quarterly and likely delayed by OEMs/carriers, leaving older devices vulnerable.
Permission Granularity	Apps request permissions upfront (e.g., "Allow access to photos once"). Background location tracking requires recurring user consent.	Granular permissions (e.g., "Allow access to camera only while using app"). However, APIs can be abused to collect data in background.
Third-Party App Stores	Not allowed (except under limited EU-mandated conditions).	Permitted, increasing **exposure to unverified apps and cyber threats.**
Sandboxing	Strict app sandboxing-apps cannot access other apps' data or OS resources without explicit permissions.	Sandboxing exists but less restrictive; apps can share data via intents or storage -malware like SharkBot exploits gaps in sandboxing
User Flexibility	Limited, **users can only install apps through Apple's system.**	High flexibility, **allowing sideloading but requiring** stronger security measures.

[21] Apple Developer. App Review Guidelines. Available at: https://developer.apple.com/support/downloads/terms/app-review-guidelines/App-Review-Guidelines-20240913-English-UK.pdf; External link account. Available at: https://developer.apple.com/documentation/storekit/external-link-account; Apple Platform Security. Operating system integrity. Available at: https://support.apple.com/en-in/guide/security/sec8b776536b/web; Goad, M. (2023, September 23). Are iPhones more secure than Android devices?. TechTarget. Available at: https://www.techtarget.com/searchmobilecomputing/tip/Are-iPhones-more-secure-than-Android-devices; Apple. About software updates for Apple devices. Available at: https://support.apple.com/en-in/guide/deployment/depc4c80847a/web; Nield, D. (2024, March 2). How to manage app permissions on your iPhone. The Verge. Available at: https://www.theverge.com/24087604/iphone-app-permissions-how-to; Installing apps through alternative app distribution in the European Union. Available at https://support.apple.com/en-in/117767; Security of runtime process in iOS and iPadOS. Available at: https://support.apple.com/en-in/guide/security/sec15bfe098e/web

[22] Prepare your app for review. Available at: https://support.google.com/googleplay/android-developer/answer/9859455?hl=en; Handling Android App Links. Available at: https://developer.android.com/training/app-links; Handle Play Integrity API error codes | Google Play. Available at: https://developer.android.com/google/play/integrity/error-codes; Piloting new ways of protecting Android users from financial fraud. Available at: https://security.googleblog.com/2024/02/piloting-new-ways-to-protect-Android-users-from%20financial-fraud.html; Mobile device security and data protection. Available at: https://www.android.com/intl/en_in/safety/; Android Authority. (2024, October 17). Phone update policies from every major company. Available at: https://www.androidauthority.com/phone-update-policies-1658633/; Permissions on Android. Available at: https://developer.android.com/guide/topics/permissions/overview; Find third-party software notices in Google for Android. Available at: Find third-party software notices in Google for Android; Application Sandbox. Available at: https://source.android.com/docs/security/app-sandbox.

3. APP STORE SECURITY: KEY MEASURES PROTECTING EUROPEAN USERS

App stores serve as the primary gateway for software distribution, placing them at the forefront of cybersecurity efforts. Both closed and open ecosystems, such as those managed by major operating system providers, implement rigorous security frameworks to mitigate risks from malware, data breaches, and fraudulent applications. While open ecosystems have made significant strides in enhancing app security, the fragmented nature of updates across third-party stores continues to pose challenges. This section outlines the key security measures implemented by app store providers to protect European users, focusing on threat detection, policy enforcement, and proactive security initiatives.

Apple's security ecosystem relies on strict app notarisation and hardware-software integration to protect user data and maintain platform integrity. However, regulatory demands under the DMA, such as opening NFC functionalities and mandating external app store links, risk undermining these safeguards. Reflecting these concerns, Apple has decided to withhold certain features in the EU due to regulatory uncertainty.[23]

To comply with the DMA, effective March 2024, Apple announced changes to iOS, Safari, and the App Store, including support for alternative app marketplaces, third-party payment processors, and non-WebKit browser engines. While these changes aim to promote competition, Apple warns they introduce increased security and privacy risks. To mitigate threats like malware and fraud, Apple will implement safeguards such as app notarisation and marketplace developer authorisations, but acknowledges that some risks cannot be fully eliminated.

Likewise, Google Play has continuously strengthened its security defences to protect users, developers, and the integrity of Android and its app ecosystem. Despite these efforts, security updates remain fragmented across the broader Android landscape. While Google Play Services delivers consistent and timely security patches, third-party app stores often do not prioritise such updates, creating gaps that can leave users vulnerable to potential exploits and security threats. Key initiatives include:

Blocking Malicious Apps

In 2024, Google blocked 2.36 million apps that violated its policies from being published on Google Play and banned approximately 158,000 developer accounts attempting to publish malicious apps. Additionally, it also prevented 1.3 million apps from obtaining excessive or unnecessary access to sensitive user data.[24] These applications were identified as violating Google's security policies, often posing risks such as malware distribution, data theft, or fraudulent activity.

[23] Apple (2024). Apple announces changes to iOS, Safari, and the App Store in the European Union. Available at https://www.apple.com/newsroom/2024/01/apple-announces-changes-to-ios-safari-and-the-app-store-in-the-european-union/?utm_source=chatgpt.com.

[24] Otuteye et al. (2025, January 29). How we kept the Google Play & Android app ecosystems safe in 2024. Google Security Blog. Available at: https://security.googleblog.com/2025/01/how-we-kept-google-play-android-app-ecosystem-safe-2024.html.

To enhance its ability to detect and remove fraudulent applications, Google employs a combination of human security experts and threat detection technology, and advanced machine learning (ML) algorithms that continuously analyse app behaviour and developer activities. This technology helps identify potentially harmful apps before they are made available to users, significantly reducing the risk of exposure to malicious software. By leveraging automated systems and human review processes, Google ensures that users can confidently download and use applications without compromising their data security.[25]

Strengthening Security Policies

Google has implemented several initiatives to support developers in creating secure applications while protecting users from vulnerabilities. One of these key initiatives is the Google Play SDK Index, a resource designed to help developers make informed decisions when selecting third-party software development kits (SDKs). By offering transparency regarding security practices and compliance with Google's policies, the SDK Index encourages developers to integrate trusted components into their applications, reducing the likelihood of security flaws.[26]

In addition to providing tools for developers, Google has reinforced its security efforts through strategic industry partnerships. The App Defence Alliance (ADA) – a collaboration with Microsoft and Meta – was established to bolster app security by sharing intelligence on emerging threats and coordinating responses to vulnerabilities. This alliance enables a more proactive approach to identifying and mitigating risks before they impact users.[27]

Regular security updates play a crucial role in keeping Android devices safe. Google continuously releases critical patches to address flaws in Android OS, Google Play services and hardware specific components and focuses on newly discovered vulnerabilities, ensuring that users receive timely protection against evolving threats. Google's Project Treble (modularising Android's core) and Project Mainline (updating core OS components via Google Play) have improved update efficiency for newer devices. By maintaining a consistent update cycle, Google's update system is strong for supported devices.

Enhancing User Protection

Google utilises Play Integrity APIs along with automatic protection resulting in 80% reduction in usage from unverified and untrusted app sources that implement the API.[28] This technology scans newly installed applications for suspicious behaviour, identifying potential security risks before they can cause harm. By analysing app permissions, code patterns, and user feedback,

[25] See, e.g., DOR (2025). How Google Uses Machine Learning Techniques to Detect and Classify Potentially Harmful Application. Available at https://www.developeronrent.com/blogs/google-uses-machine-learning-techniques-detect-classify-potentially-harmful-application.

[26] See, e.g., Google (2025). Google Play SDK Index. Available at https://play.google.com/sdks.

[27] See, e.g., The Linux Foundation (2023, November 8). App Defense Alliance Migrates Under Joint Development Foundation with Google, Meta, and Microsoft as the Steering Committee. Available at https://www.linuxfoundation.org/press/app-defense-alliance-migrates-under-jdf-with-google-meta-microsoft-as-steering-committee?

[28] Mathur, C. (2025, January 29). Google Play Protect defended your sensitive data from over a million apps in 2024. Android Police. Available at: https://www.yahoo.com/tech/google-play-protect-defended-sensitive-180011716.html

Google's AI-driven systems provide an additional layer of defence against malicious software.[29] In 2023, Play Protect prevented 200,000 unique apps from disrupting 10 million devices by blocking 36 million dangerous installations.[30] Recognising that security begins at the point of entry, Google has implemented stricter developer onboarding procedures to prevent bad actors from infiltrating the Play Store. By enforcing rigorous identity verification and requiring adherence to Google's security standards, these measures help ensure that only legitimate developers can publish applications on the platform. This proactive approach significantly reduces the likelihood of deceptive or harmful apps being distributed to users.[31]

For applications that require a higher level of security, such as VPN services, Google has introduced a labelling system that enhances user trust. VPN apps that successfully complete a security review through the Mobile App Security Assessment (MASA), a program under the App Defence Alliance, receive a designation indicating their compliance with security best practices. This initiative helps users make informed choices when selecting privacy-focused applications, reinforcing confidence in the Play Store's commitment to security.[32]

4. CONCLUSIONS AND POLICY RECOMMENDATIONS: ENSURING SECURITY WHILE ENFORCING THE DMA

While the DMA's objectives to enhance competition and consumer choice are commendable, these goals must be balanced with cybersecurity priorities to avoid negative consequences.

The DMA aims to enhance competition, but overenforcement of it will weaken cybersecurity. Forcing open linkouts in in app stores would expose users to new threats. In the case of Google Play, Android's openness limits Google's control – developers can promote rival app stores like Huawei AppGallery, and Google cannot mandate Play Store pre-installation or restrict sideloading. Article 5(4) risks further fragmenting Android, undermining Google's ability to monetise and maintain security standards.

DMA enforcement must not create dangerous loopholes that weaken security in the name of competition. Instead, policymakers should work alongside technology leaders, cybersecurity specialists, and industry stakeholders to strike a balance between competition policy and best security practices. By doing so, the EU can protect both European businesses and consumers, ensuring that regulatory decisions enhance rather than compromise cybersecurity.

In conclusion, the DMA and its enforcement must balance promoting competition with safeguarding cybersecurity. While expanding app distribution fosters innovation, enforcement should not compromise user safety. To achieve this, we recommend:

[29] Google Security Blog (2024). Safer with Google: New intelligent, real-time protections on Android to keep you safe. Available at https://security.googleblog.com/2024/11/new-real-time-protections-on-Android.html.

[30] Mathur, C. (see note: 24).

[31] See, e.g., Google (2024). 7 ways we're incorporating security by design into our products and services. Available at https://blog.google/technology/safety-security/google-secure-by-design-pledge/.

[32] Google (2025). Helping users find trusted apps on Google Play. Available at https://android-developers.googleblog.com/2025/01/helping-users-find-trusted-apps-on-google-play.html.

1. **Ensuring Technology Neutrality:** The application of the DMA should be technology- and architecture-neutral, fostering competition between different ecosystem models, all of which make significant efforts to enhance security to build trust in their platforms.

2. **Upholding Regulatory Coherence:** The EU should align the DMA with its broader cybersecurity framework, ensuring that competition policies do not conflict with existing regulations aimed at enhancing digital security, such as the NIS2 Directive or the Cyber Resilience Act.

3. **Recognising Differences in Operating Systems and Platforms:** Different operating systems have distinct architectures and security models, requiring different competition and security policies. A one-size-fits-all approach could weaken consumer protection.

4. **Maintaining Security Measures:** Operating system providers, regardless of their business models, should retain the ability to implement security measures – such as blocking unvetted third-party linkouts – to mitigate malware, fraud, and data breaches. If external links are mandated, they should lead only to verified, secure platforms.

5. **Exempting Providers from DMA Penalties for Justified Security Actions:** Providers should be exempt from penalties if they can demonstrate that restrictions, such as blocking a third-party app store, were necessary to mitigate imminent, evidence-based cybersecurity risks like active exploit chains.