CENTER FOR
CYBERSECURITY
POLICY AND LAW

February 12, 2025

VIA ELECTRONIC SUBMISSION

RE: Comment on the Strategic Market Status Investigations into Apple's and Google's mobile ecosystems

To the relevant members of the Competition and Markets Authority,

Thank you for the opportunity to comment in the *Strategic Market Status Investigations into Apple's and Google's mobile ecosystems*. I am writing to share the view of the Center for Cybersecurity Law & Policy (CCPL) in this proceeding, as well as our report, *Trusted App Stores: Protecting Security and Integrity* (the CCPL Trusted App Store report). While this report addresses the implementation of the European Union's Digital Markets Act, there are many common themes that speak to this investigation as well. We appreciate and share your desire for a vibrant and competitive mobile ecosystem. However, we would like to share our concerns about the potential cybersecurity impact of potential interventions, particularly ecosystem requirements for app distribution and interoperability. We urge the Competition and Markets Authority (CMA) to consider these impacts and to find a balance that protects both competition and security.

We urge the CMA to carefully balance the priorities of competition and innovation with safeguarding cybersecurity in these digital markets, both for the ecosystem broadly and its users. The CCPL Trusted App Store report discusses how effective cybersecurity and safety work in app stores and the mobile ecosystem broadly foster effective competition. These protections are critical to ensure the new digital markets competition regime delivers its intended benefits without compromising user safety. A balanced approach can help ensure that users, developers, and the rest of the mobile ecosystem are not negatively impacted by security threats - and continue to ensure a growing, competitive mobile ecosystem.

As outlined in the CCPL Trusted App Store report, a proliferation of ways to install apps will overwhelm users and open numerous avenues for bad actors to exploit them. In turn, this would create confusion about the trust, safety, and security processes that third-party app stores may or may not implement and whether they are effective. This confusion - and the likely influx of questionable or malicious app stores and apps - would significantly impact the user experience and safety of citizens, undermining both the security and competition of the mobile ecosystem.

A balanced approach to creating competition can maintain the security and safety progress that we have witnessed in the mobile ecosystem, but requires action from companies and users themselves, in partnership with effective and measured policies from the CMA, to ensure the

protection of these new marketplaces. The CCPL Trusted App Store Report contains recommendations to help ensure that users can continue to trust the mobile ecosystem and potential security mitigations for users and enterprises. Specifically, we encourage CMA to consider and integrate comprehensive security measures to address the risks associated with greater interoperability and increased mechanisms for app distribution in the iOS ecosystem. We urge you to carefully promote competition while preserving the trust and safety that users expect from digital services.

We welcome the opportunity to discuss these issues further with your team and are grateful for your willingness to engage in this vital dialogue. Please let me know if you have any other questions.

Sincerely,

About the Center for Cybersecurity Policy & Law:

The Center for Cybersecurity Policy & Law is an independent organization dedicated to enhancing cybersecurity worldwide by providing government, private industry, and civil society with practices and policies to better manage security threats.

Established in 2017 as a 501(c)(6) nonprofit, the Center combines policy expertise with convening power to bring industry leaders together with policymakers, form coalitions, and launch initiatives that produce real-world outcomes.

Applying a consensus-oriented, risk management-based approach, the Center seeks to demystify the complexities and dispel the confusion around cybersecurity by promoting pragmatic solutions and policy recommendations drawn from the perspectives and practices of those on the frontlines of securing digital infrastructure and information systems.

Trusted App Stores: Protecting Security and Integrity

February 2024

[redacted]

[redacted]

CENTER FOR CYBERSECURITY POLICY AND LAW

Table of Contents

Executive Summary

As the European Union (EU) implements new policies and regulations for their digital market, it must carefully balance economic considerations alongside access, privacy, and security. Unfortunately, the mobile app store provisions of the Digital Markets Act (DMA) could undermine foundational security controls that have made the mobile phone ecosystem so trustworthy and resilient. The Center for Cybersecurity Policy & Law is concerned that a proliferation of ways to install apps will be overwhelming to users and open numerous avenues for bad actors to exploit them. This is not to suggest that there is nothing that can be done to protect users, but it will take action from companies and the users themselves to make sure that they are protected in ways they have not had to in the past. This paper outlines potential risks to EU citizens, their devices and data, as well as approaches to mitigating those risks. We conclude with recommendations to help regulators and policymakers ensure that users can continue to trust the mobile ecosystem, and how to mitigate potential security implications for users and enterprises. We hope this paper will also provide insights for other countries as they look to foster competition in their own digital markets while protecting the security and privacy of their citizens.

About the Center for Cybersecurity and Law

The Center for Cybersecurity Policy & Law is an independent organization dedicated to enhancing cybersecurity worldwide by providing government, private industry, and civil society with practices and policies to better manage security threats. Established in 2017 as a 501(c)(6) nonprofit within Venable LLP's Cybersecurity Services group, the Center combines policy expertise with convening power at global, national, and local levels to bring industry leaders together with policymakers to form coalitions and launch initiatives that produce real-world outcomes. Applying a consensus-oriented, risk management-based approach, the Center seeks to demystify the complexities and dispel the confusion around cybersecurity by promoting pragmatic solutions and policy recommendations drawn from the perspectives and practices of those on the frontlines of securing digital infrastructure and information systems.

Introduction

In an increasingly connected world, we often use apps on our mobile phones to interact with a rich ecosystem of services, information, and resources. The benefits of our mobile phones are widely acknowledged:[1] they are our windows to the world, track our health, share with our friends, purchase goods, and manage services. And accordingly, we spend a lot of time in mobile apps - four to five hours a day, or more.[2] It is critical that our devices and apps remain secure and trustworthy.

Studies suggest that within the United States, 81% of consumers, aged 18-34, feel the connected devices they own are secure.[3] People have good reason to trust their mobile devices and apps, thanks to the efforts of operating system developers and app store to secure these ecosystems.

For our 2021 paper *Mobile Future: Pathways to Continued Improvement in Mobile Security and Privacy*,[4] we discussed mobile security with twenty-three cybersecurity experts from industry, academia, and civil society, and found that "while new threats to mobile devices continue to arise, the protections in place are generally working better than in other areas of cybersecurity." The consensus from our focus group was that the mobile environment benefitted from built-in security and privacy protections at the operating system (OS) and app store level, significantly reducing the onus on users to protect themselves.

That paper, only three years old, was written in the context of current mobile architectures and security capabilities from reputable operating system developers and their trusted official app stores. Over the past decade the mobile ecosystem has gotten progressively safer - but the app installation provisions of the European Union's competition-focused DMA[5] may send the ecosystem backwards instead of continuing this security progress. We need to work together to ensure that we maintain this security progress.

Provisions of the DMA requiring that operating systems allow app installation from additional sources have the potential be overwhelming to users, a challenge to enterprise administrators implementing mobile device management, and could open new avenues for bad actors. Mitigating these risks will require supporting mobile operating system gatekeepers to balance the intent of the DMA while taking reasonable approaches to mitigate the risks that will accompany a more open ecosystem.

This paper will briefly outline the app store provisions within the DMA, the mobile ecosystem threats exacerbated by those provisions, and make a brief examination of how first-party app store and mobile OS owners have historically combatted these

---

[1] https://www.pewresearch.org/internet/2019/03/07/majorities-say-mobile-phones-are-good-for-society-even-amid-concerns-about-their-impact-on-children/

[2] https://techcrunch.com/2022/08/03/mobile-users-now-spend-4-5-hours-per-day-in-apps-report-says/?guccounter=1

[3] https://staysafeonline.org/wp-content/uploads/2022/07/Cybersecurity-Awareness-Month-2020-Results-Report.pdf

[4] https://assets.website-files.com/62715f02a51b614ce64867fd/628e6ba29361afc22807be6b_mobile-future-pathways-to-continued-improvement-in-mobile-security-and-privacy.pdf

[5] https://eur-lex.europa.eu/eli/reg/2022/1925

threats. This paper will make a case for the kinds of DMA implementation approaches that EU member states should support to ensure that unprepared end users are not suddenly on the hook for the security of the mobile ecosystem and their devices.

The DMA text references potential avenues to protect users, including both technical and contractual mechanisms; additionally, legislators and regulators should support the role of operating system developers to protect users through app reviews, enhanced malware protection, transparency requirements, and adjustments to permissions and security models built into mobile device operating systems. It is important to ensure that we work together to ensure a vibrant, innovative mobile ecosystem. We urge policymakers to emphasize the importance of security in DMA's implementing acts and as gatekeepers work to establish their compliance.

DMA App Store Provisions

By March of 2024, companies covered under the definition of "gatekeeper" who operate "core platform services" will be subject to DMA provisions related to their app stores and mobile OS interactions with third-party app stores and apps. Gatekeepers are those companies, as designated by the European Commission, who have a significant impact on the European market and provide a service that intermediates the relationship between businesses (e.g., app developers) and end users (e.g., users of mobile phones installing apps).[6] The intention of the DMA is to make it easier for smaller European companies to compete with companies that may have a more "entrenched" position in the market.

DMA provisions require that mobile operating systems allow the installation of apps from non-gatekeeper app stores or via other methods, and that operating systems allow the same system access and tooling to first- and third-party apps.

The heart of these provisions include:

- *Section 6.4: The gatekeeper shall allow and technically enable the installation and effective use of third-party software applications or software application stores using, or interoperating with, its operating system and allow those software applications or software application stores to be accessed by means other than the relevant core platform services of that gatekeeper.*

- *Section 6.7: The gatekeeper shall allow providers of services and providers of hardware, free of charge, effective interoperability with, and access for the purposes of interoperability to, the same hardware and software features accessed or controlled via the operating system or virtual assistant [...]. Furthermore, the gatekeeper shall allow [...] effective interoperability with, and access for the purposes of interoperability to, the same operating system, hardware*

[6] As of publication, Apple's iOS operating system and Google's Android operating system are considered core platform services. Microsoft's Windows desktop PC operating system is also considered a core platform service but is outside the scope of this paper. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328

> *or software features, regardless of whether those features are part of the operating system, as are available to, or used by, that gatekeeper when providing such services.*

These DMA provisions, when combined with other European Union laws, will effectively require gatekeepers to allow easier installation of third-party apps and app stores on mobile devices, allow easier access to third-party app stores by mobile users, and grant third-party developers and apps the same access, interoperability, and functionality with mobile OS' that gatekeepers currently enjoy.

In addition to these provisions -- and highlighting an awareness of the security and privacy risk posed by the "opening up" of the mobile ecosystem -- there is an underemphasized security caveat. Recital 50 of the DMA states that the additional access provided to third-party apps and app stores should not undermine user and device security. However, the DMA does not outline how it expects operating systems to protect mobile devices and users given restrictions on how operating systems can differentiate or curtail access to apps. If implemented without careful consideration, the above provisions of DMA could exacerbate the current mobile threat ecosystem.

The Mobile Threat Ecosystem

Combatting mobile malware is a priority for mobile OS developers and for organizations around the world. Despite their successful and protective security architecture, mobile devices are a tempting target due to their ubiquity, the fact that they accompany us throughout our day, and because they're such a core part of our lives and sit in the middle of so many of our digital interactions.

Mobile threats have also grown as operating systems became true platforms rather than closed ecosystems, and mobile OS developers and reputable app store operators have been working to curb threats ever since through OS architecture design choices sandboxing apps and data, app moderation, app functionality and quality checks, and increasingly granular permission models. CrowdStrike's 2019 Mobile Threat Landscape Report found that mobile platforms are increasingly targeted by criminals, and that less-skilled adversaries now have access to proof-of-concept mobile malware that allows them to easily try to gain access to mobile devices.[7]

Primary Mobile Threats

There are myriad threats for, and to, the mobile ecosystem as malicious and opportunistic actors both look for any way to leverage these incredibly popular platforms. As gatekeepers and policymakers implement the DMA, they must keep in mind ways to minimize these threats.

[7] https://www.crowdstrike.com/resources/reports/mobile-threat-report-2019/

Malicious apps have long been the most significant threat to mobile devices given their potential to directly interface with sensitive stored data and the mobile device's core functionality. According to a Nokia[8] and Kaspersky studies,[9] most mobile malware makes it onto mobile devices via trojanized apps. These apps pretend to be things that people actually do want to install, from a flashlight app to free versions of expensive software - but the trojanized app is hiding unwanted behaviors such as harvesting sensitive information or credentials.[10] This is possible because the apps ask for permissions they wouldn't need for its surface level function, like a flashlight app that requests location data or contacts stored on the phone.[11] The user installs what seems to be a benign app or game, usually for free, but opens their device and data to malicious actors. Check Point has reported an increase in these apps, especially those that purpose to offer a free trial or extra functionality.[12] They note that there is risk in trusting the familiar, as many of these apps leverage familiar brand and product names – but then steal data, credentials, or add the device to a botnet.[13]

These malicious apps often successfully conceal their true nature. There's a proliferation of trojanized apps -- including hack tools, accessware, spyware, adware, dialers, and joke programs -- that have annoying or harmful behavior that a user doesn't want.[14] There are even malware-as-a-service providers that create apps to take over accounts and join mobile devices to botnets.[15]

Some of these apps are also highly targeted. For example, several instant loan app scams have been circulating across India and other countries in Asia, Africa, and Latin America. After installation, the app may well provide a loan, but also harvests information from the phone -- both information about the user and other data on the phone, including nude photographs - which are then be used to harass, intimidate, and extort.[16]

With the primary mobile threat identified, the natural question is, "but how do these malicious apps get installed?" First-party app stores like Google Play Store and Apple App Store are not flawless in keeping out bad apps, but most apps on their stores are benign, due to their efforts to keep their stores safe. The riskiest vectors for malware come from third-party app stores and

---

[8] https://www.nokia.com/networks/security-portfolio/threat-intelligence-report/

[9] https://securelist.com/mobile-malware-evolution-2020/101029/

[10] https://www.mcafee.com/blogs/mobile-security/mobile-spyware/, https://www.appdome.com/dev-sec-blog/mobile-payment-security/

[11] https://blog.avast.com/flashlight-apps-on-google-play-request-up-to-77-permissions-avast-finds

[12] https://resources.checkpoint.com/report/2023-check-point-cyber-security-report

[13] https://www.verizon.com/business/resources/T9bc/reports/mobile-security-index-report.pdf

[14] https://docs.broadcom.com/doc/istr-23-03-2018-en

[15] https://www.androidpolice.com/android-botnet-trojan-steal-banking-data/

[16] https://www.bbc.co.uk/news/world-asia-india-66964510

sideloading. While accurately quantifying the amount of risk posed by each method is exceptionally difficult, some studies do suggest substantial risks to users.

Third-Party App Stores

While some studies have suggested that major third-party app stores *can* be safe in comparison to first-party app stores, like the Google Play Store, evidence suggests that third-party stores increase the security and privacy risk to mobile users – but that's not because they aren't associated with the operating system. Instead, they generally do not or cannot take the same diligence in policing their apps - likely one of the reasons that major mobile OSs have not historically allowed third-party app stores by default.[17] And there are some examples of app stores that are themselves intended to install malicious apps.[18] In a 2021 focus groups, CrowdStrike noted that the majority of mobile malware is distributed from third-party sources that do not perform comprehensive checks of applications they provide.[19]

While quantifying the exact risk is difficult, one 2020 study found that Android users of "other top alternative markets'' were five times riskier on average, and upwards of nineteen times more likely to come across malware or a malicious app than those that used the Google Play store.[20] Additionally, cybersecurity company Symantec reported in 2018 that fully 99.9% of mobile malware they discovered was hosted on third-party app stores.[21]

This has led to a consensus among security experts and regulators that downloading apps from most third-party app stores is far riskier than from a trusted first-party. Major government and private organizations advise against downloading apps from unofficial and untrusted sources, including warnings at various times coming from ENISA, Europol,[22] the U.S. NSA,[23] the U.S. FTC tasked with consumer protection, the U.K. National Cyber Security Centre,[24] India's CERT-In,[25] U.S. DHS's CISA[26], the

---

[17] https://citrixready.citrix.com/content/dam/ready/partners/wa/wandera/wanderas-web-gateway-for-mobile/mobile-threat-landscape-2020-whitepapers.pdf

[18] https://www.makeuseof.com/what-are-the-dangers-of-third-party-app-stores/#:~:text=Many%20malicious%20actors%20have%20created,hidden%20trackers%20and%20malicious%20code.

[19] https://www.centerforcybersecuritypolicy.org/insights-and-research/mobile-future-pathways-to-continued-improvement-in-mobile-security-and-privacy

[20] https://arxiv.org/pdf/2010.10088.pdf

[21] https://docs.broadcom.com/doc/istr-23-03-2018-en

[22] https://www.europol.europa.eu/sites/default/files/documents/infographic_-_apps.pdf

[23] https://media.defense.gov/2020/Jul/28/2002465830/-1/-1/0/MOBILE_DEVICE_BEST_PRACTICES_FINAL_V3%20-%20COPY.PDF

[24] https://www.ncsc.gov.uk/files/Protecting-devices-from-viruses-malware-infographic.pdf

[25] https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2020-0013

[26] https://www.cisa.gov/sites/default/files/publications/CEG_Mobile_Device_Cybersecurity_Checklist_for_Organizations_0.pdf

Commerce Department's NIST,[27] New Zealand's CERT NZ,[28] and others. Despite this, studies have shown that consumers will use third-party app stores if the apps are free or have modified versions of well-known games and apps.[29] Users aren't keeping their security in mind – they just want to get that app that sounds too good to be true fast and preferably free.

Sideloading

By comparison, sideloading does not require any kind of traditional app storefront and a sideloaded app may be distributed or advertised with little background context, no vetting, and false or misleading claims around security and authenticity. There is no intermediary to perform this diligence, as sideloading can happen from anywhere – a website, a message attachment, or an obscured link.

Sideloading requires the individual to trust a third-party who may not have the reputation, experience, or means of ensuring that the app has not been tampered with, though users don't think about that when they find a new game they want to try. While many third-party websites and stores may be safe, a user is unlikely to find the same level of transparency when it comes to how the app has been vetted and what permissions it may seek, and it is much simpler to pretend to be something you are not without the infrastructure of a reputable app store.

Sideloading is the riskiest method for users to acquire mobile apps. While that risk has been traditionally offset by the fact that side loading often requires a level of technical expertise that many end users don't possess, if mobile operating systems allow sideloading by default that friction will disappear. Even well-informed end users who sideload are often ultimately trusting unknown or questionable developers and app stores, and no amount of technical knowledge is likely to credibly lower the risk unless you only downloaded directly from well established companies.

The Failure of End User Responsibility

Studies show that a user's security decisions do not necessarily correlate with their knowledge of security threats.[30] Despite the very real harm that malicious apps can cause, mobile users are rarely willing to spend considerable time to look critically at the permissions that apps request, and often do not understand the implications if they try.[31] And when users are interrupted with security warnings, they overwhelmingly ignore it.[32]

---

[27] https://www.nccoe.nist.gov/sites/default/files/legacy-files/mtc-nistir-8144-draft.pdf

[28] https://www.cert.govt.nz/individuals/guides/keep-mobile-phone-safe-secure/

[29] https://www.jamf.com/blog/what-are-third-party-app-stores-and-are-they-safe/

[30] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5352308/

[31] https://link.springer.com/chapter/10.1007/978-3-031-35822-7_36

[32] https://news.sophos.com/en-us/2016/08/19/why-people-ignore-security-alerts-up-to-87-of-the-time/

Many users don't even take basic security measures for their mobile devices - for example, one study found that 40% of users reported that they don't update their operating system and apps unless it's convenient, and 28% don't use a screen lock.[33] Another study found that three quarters of smartphone users believe that apps they download from app stores are inherently secure,[34] making them unlikely to be skeptical of them. That study even found that app users could not, or did not care to, differentiate the level of security provided by various app stores. Additional recent studies confirm that users care about security risks but lack the knowledge and skills to effectively protect themselves - and often don't even attempt to do so.[35]

While we hope that users will take a more active role in protecting themselves online, best practice is increasingly to remove as much of that burden from them as possible. National cyber strategies and government best practices increasingly seek to shift the balance away from users, and put the onus of protecting devices, data, and people on the companies that are distributing them. In 2023, national cybersecurity agencies from the United States (CISA), Czech Republic, Israel, Singapore, Korea, Norway, OAS/CICTE CSIRT Americas Network, and Japan (JPCERT/CC and NISC) jointly released guidance on shifting the balance of risk away from end users.[36] Many organizations in both the public and private sectors also choose to use Mobile Device Management (MDM) to ensure that only approved apps are installed on devices that also have access to sensitive data or apps, and these tools may in the future allow administrators to determine which app stores are allowed.

Given the extent and complexity of the above risks, it's irrational to expect end users to suddenly have the requisite awareness and understanding of mobile security and privacy, including how to protect themselves via layered security, configuring an optimal combination of settings for their accepted risk, and other methods simply aren't viable at scale. End users are likely to assume that universally available app stores are safe. There are other approaches – but they will require protections like the ones that gatekeepers have already put in place in their own app stores.

How Google and Apple Combat these Threats

Many first-party app stores, like those from Apple App Store and the Google Play Store and others that have not been determined to be gatekeepers under the DMA, take extensive measures to mitigate the risks identified above through policies and processes designed to screen new and updated apps for malware or significant changes to original app functionality. Both Apple and Google have created policies and processes that extend from the developer, through their official app stores, and on to consumers. While no app store is completely secure, these efforts have resulted in the Google Play Store and Apple App Store earning a reputation for consumer trust and safety through years of investment and learning to inform their approaches to protecting users.

---

[33] https://www.pewresearch.org/short-reads/2017/03/15/many-smartphone-owners-dont-take-steps-to-secure-their-devices/

[34] https://www.sciencedirect.com/science/article/pii/S0167404812001733#fn6

[35] https://dl.acm.org/doi/fullHtml/10.1145/3491102.3517504#sec-21

[36] https://www.cisa.gov/resources-tools/resources/secure-by-design

Leading first-party app stores like the Apple App Store and Google Play Store achieve security through the implementation of processes like setting baseline requirements and guidelines, requiring self-attestations, and by reviewing the apps.[37] App developers must successfully meet the various security, privacy, and transparency requirements for their apps in order to be featured on one of these app stores. This may include ensuring that an app does what is advertised, seeks only appropriate permissions, and has functional privacy policies in place. Apple and Google's app stores also require transparency in their app store listing, including permissions that the app uses and information about data collection.[38], [39]

First-party app stores may also have additional protections in place outside of reviewing the app itself, such as vetting developer accounts. For instance, the Google Play Store analyzes "a developer's Google account, actions, history, billing details, device information, and more" to identify potential red flags.[40]

When it comes to reviewing an app submission, first party app stores can take any number of actions to ensure its function: the store may review app developer attestations, apply various automated reviews, and have a human reviewer manually review the app. These reviews may use a variety of tools and techniques to perform static and dynamic reviews that search for malware or other potentially harmful or unwanted aspects. Furthermore, beyond the routine inspections of newly submitted apps, first-party app stores, like Apple's, review app updates to ensure that any new functionality remains safe. Finally, first party app stores tend to trigger reviews based on consumer or security researcher complaints or notices that an app is engaging in unwelcome behaviors.

If an app fails to meet and maintain the necessary requirements and guidelines for inclusion in the app store, the app will typically be removed. The scale of these issues is notable, with Apple detailing that they rejected over 1.5 million app submissions and removed more than 186,000 apps from their app store in 2022.[41] These removals promote a safe and trusted app store environment, keep end users from harm, and incentivize bad actors to look for other more fruitful means of infecting devices.

At the consumer level, Apple and Google have made significant efforts to make their security and policy protections and requirements easily accessible and understandable by users of their app stores. In addition, both have sought to create more transparency with regards to the permissions that vetted apps seek so consumers can make informed decisions on the level of privacy and security they desire beyond the official app store baseline. The Google Play Store has even begun displaying a

---

[37] https://developer.apple.com/app-store/review/guidelines/, https://play.google.com/about/developer-content-policy/

[38] https://support.google.com/googleplay/android-developer/answer/10144311?hl=en

[39] https://developer.apple.com/app-store/user-privacy-and-data-use/#:~:text=In%20order%20to%20submit%20new,websites%20owned%20by%20other%20companies.

[40] https://developers.google.com/android/play-protect/cloud-based-protections

[41] https://www.apple.com/legal/more-resources/docs/2022-App-Store-Transparency-Report.pdf

badge on apps that have completed an independent security review.[42] These processes and policies have proven to be effective, but they are significant investments.

Security for Mobile App Stores is an Investment

As established above, placing the onus of security on end users is ineffective, and goes against cybersecurity best practices that increasingly promote policies and processes to ensure that the user is protected by default. While large well-resourced entities like Google and Apple have the expertise, resources, and willingness to effectively do so, few others can say the same.

The types of protections noted above, which are rarely if ever implemented to the same degree by third-party app stores, weed out a majority of malicious, low quality, and deceptive apps. Third-party app stores do not have the same level of resources, experience, knowledge of the platform and OS, or incentive to protect their app store or vet their hosted apps as first-party app stores. Furthermore, third-party app stores may look to differentiate themselves from the larger established stores by being more permissive of apps that would otherwise be deemed unwelcome. On the other side of the coin are first-party app stores, which spend considerable resources to improve the security of apps on their marketplace.

A Roadmap for DMA Implementation

Requiring mobile operating systems to allow third-party apps will unavoidably have negative effects on the privacy and security of the mobile ecosystem, but there are ways to safely allow users greater access to third-party apps and app stores while also giving third-party app developers greater access to OS-level functionality. As we have indicated above, and as first-parties like Apple have attested, compliance with the DMA is all but certain to increase the prevalence of "malware, fraud and scams, illicit and harmful content, and other privacy and security threats."[43] However, lawmakers and policymakers can mitigate these issues with constructive implementation guidance that enables gatekeepers to protect their consumers.

EU member states should be willing to support first-party app store and mobile OS owners, as well mobile device users, by supporting:

- Gatekeepers should undertake baseline app reviews regardless of distribution channel. This may require new mechanisms built into operating systems, or contracts with app stores. There may also be a way to use certifications and third-party evaluations to demonstrate that apps are safe.
- Policymakers should consider app description notices regarding basic functionality and essential information, to help users and others understand how apps work and what they are intended to do.
- Operating systems may implement enhanced mobile protections to prevent malware from harming the security and integrity of the mobile device, including additional tools to sandbox and protect apps from each other and to protect the operating system, user data, and device hardware from malicious apps. These tools could include MDM tools for enterprise administrators.
- Gatekeepers should put in place technical and contractual controls for third-party app stores in order to ensure that they can be trusted. Each gatekeeper is likely to choose a different balance between different mitigations, but they

[42] https://security.googleblog.com/2022/12/app-defense-alliance-expansion.html

[43] https://www.apple.com/newsroom/2024/01/apple-announces-changes-to-ios-safari-and-the-app-store-in-the-european-union/

should have a broad set of options to protect the device and users that can be used to protect users as they work to comply with the DMA.

- Gatekeeper mobile companies need clear guidance that they can protect their users, and be given adequate time to conceptualize, build, test, and prove out new systems to secure their users.
- Regulators should pay attention to security and integrity concerns in both apps and app stores and recognize that not all apps and stores are created equal. They should support the development of mechanisms to assess and ensure that app and app store developers behave responsibly, and that they can be held accountable if they do not.
- Gatekeepers developing mobile operating systems need to have the flexibility to adjust the permissions and security models, and how they operate, in order to ensure that developers cannot take advantage of the changing ecosystem. Policymakers must protect the ability of app stores and device operating systems to evolve the kinds of security mechanisms and limitations that are available to integrate into their ecosystem.
- Policies that address mobile ecosystems must not weaken the security of those ecosystems. Policymakers should ensure that the security and privacy of mobile platforms continues to improve, and that both are built into platforms and apps from the start. Proposals that threaten the progress that has been made should be reconsidered.
- Policymakers must be realistic about what security responsibilities and burdens users are willing and equipped to take on. Studies note that security awareness does not correlate with making good security decisions.[44]
- Policymakers should support risk-based practices for mobile devices, rather than mandating particular practices around how mobile devices operate and what apps can be installed.

Conclusion

With the DMA passed into law, and gatekeepers working to ensure their compliance, we are entering a pivotal transition for the mobile ecosystem. The Center for Cybersecurity Policy and Law hopes that policymakers and gatekeepers, and the rest of the mobile ecosystem, can work together to keep users and their mobile devices safe and secure. Policymakers should consider the security impact to companies, the ecosystem, and consumers. While the impact of many of these elements of existing app store review and oversight are difficult to quantify, the investments that app store developers make to protect their users should be recognized and rewarded. When app store owners and developers take security and privacy enhancing actions, users benefit in ways they aren't aware of.

There is no perfect system that protects users from all mobile malware, but we know how to significantly decrease the number of unwanted or malicious activities that users must consider.

[44] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5352308/