App Stores and Mobile Ecosystems

Discussion with Working Group
Digital Markets Competition Headquarters
18 October 2022

Dick Rinkema
Chief Counsel, Asia Competition Law & Policy
Microsoft Corporation

Introduction

- Microsoft will discuss the benefits of an open platform approach
- Microsoft will offer comments based on our experience on mobile platforms relating to:
    - Platform operator requirements that all native apps be distributed through proprietary app store
    - Requirements that platform operators’ proprietary payment processing systems be used for in-app purchases
    - Requirements that proprietary browser engines be used for browser and web app development, and issues limiting web app support
- Questions and discussion

Benefits of open platform approach

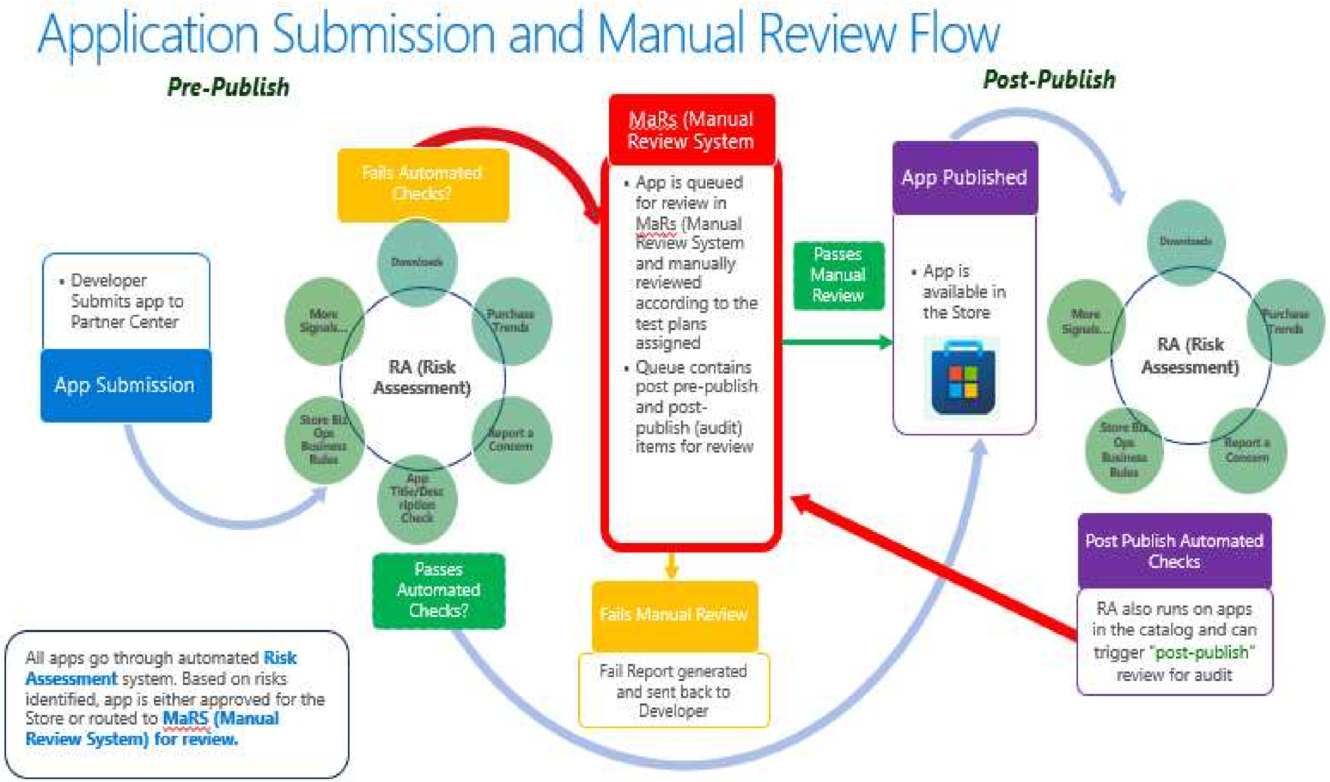
- Windows OS is an open platform: developers can offer apps directly, through third party app stores, or via the Microsoft Store on Windows
- Third party stores may be offered directly (e.g., Steam), or via the Microsoft Store on Windows (e.g., Amazon)
- Developers choose how to monetize their apps whether they are on the Microsoft Store or not – they can use their own IAP systems, a third party system, or use Microsoft's system
    - Developers do not have to offer Microsoft's IAP system alongside alternative systems
- Microsoft does not prevent developers from outlinking to alternative payment systems
- If developers do not use Microsoft's IAP system, they do not pay any fees to Microsoft
- This approach offers developers the ability to connect directly to their users and innovate freely – benefitting developers and users and ultimately, the Windows platform

A principled approach to app stores

- Microsoft’s Open App Store Principles, announced in February 2022:
  - All developers may access our app store while meeting standards for quality, safety, security, and privacy
  - We will apply the same standards to our own apps that we apply to competing apps
  - We will not use non-public information or data from our store to compete with developers’ apps
  - We will treat apps equally and with fairness and transparency as to promotion and marketing
  - Developers will retain choice as to payment systems; will not be required to provide us with better terms than competing app stores; will not be disadvantaged if they use an alternative payment system; and may communicate directly with their customers through their apps, including for pricing terms and product and service offerings
- These Principles apply to the Microsoft Store on Windows; most apply to the Xbox Store and we are working to adapt our Xbox business model to implement them all over time
- We believe this approach better serves our users and creators and will expand app markets

An open approach does not sacrifice security

- Microsoft's approach is not dependent on "guarding the gate"
- Microsoft engages in pre-publication review and post-publication risk management. Security achieved through multiple layers of protection: (i) architecture, (ii) robust review and certification, (iii) ratings, and (iv) remediation
- Apps and app stores on the Microsoft Store must have their own documented security policies and review processes
- Developers are required to receive security reports from Microsoft and respond quickly to any issues



Application Submission and Manual Review Flow

- Developer Submits app to Partner Center

- App is queued for review in MaRs (Manual Review System and manually reviewed according to the test plans assigned
- Queue contains post pre-publish and post-publish (audit) items for review

- App is available in the Store

Fail Report generated and sent back to Developer

RA also runs on apps in the catalog and can trigger "post-publish" review for audit

All apps go through automated Risk Assessment system. Based on risks identified, app is either approved for the Store or routed to MaRS (Manual Review System) for review.

Security and privacy in an open mobile platform

A minimum set of restrictions and requirements that preserve quality, security and privacy, and that are not unnecessarily burdensome, could be developed.

- Primary app stores could impose contractual requirements on alternative app stores:
    - Requiring compliance: adopting security policies and review processes, providing security reports
    - Enforcing remedies: ultimately, alternative app stores could be “taken down” if a threat is identified and not addressed by the alternative app store
- Operators could apply the same approach to alternative app stores as is currently taken in their developer programs.
- Operators could approve trusted partners (e.g. Microsoft, EA Play, Ubisoft) to certify and distribute app stores and apps.
- Operators could “containerize” apps so that they only have access to those parts of the device that are exposed to their container.
- Adopt the “notarization” model used in some desktop OS, where security measures are imposed by the operating system rather than the app store.
- Promote the adoption and verification of good software development practices.

Mandatory use of App Store

- Mandating the use of a platform operator’s app store limits competition:
  - Alternative app stores may offer a better user experience
  - Alternative app stores may offer more attractive terms to developers
  - Alternative app stores may offer better pricing for users
- The quality, security and privacy concerns raised are overstated
  - Alternative app stores can also compete on security, privacy, and quality
  - Consumers would rapidly abandon any unreliable app store
  - Platforms can require compliance with their standards and enforce them, including with take-downs
- Microsoft is already managing the quality, security and privacy risks
  - Microsoft permits alternative app stores (e.g., EA Play Store, Epic Store and Ubisoft Store) on the Microsoft Store
  - Reputable individual alternative app stores take quality, security and privacy seriously
  - Microsoft seeks to foster a cooperative relationship with alternative app stores to address these issues, including working together on engineering challenges

Web apps as an alternative to native apps on app stores

Web apps are not currently viable alternatives to native apps on mobile devices:

- Native apps offer greater functionality than web apps (e.g. push notifications, data storage, GPS, speed)
- Notwithstanding improvements made to certain browser engines, native apps continue to be technically constrained and cannot access key hardware functionality on operators' devices
- Web apps do not have a centralised point of distribution such as an app store, making it difficult for users to find (or "discover") them
- Users must use an operator's browser to install web apps on the operator's OS home screen

Mandatory use of payment processing systems

- Payment processing is a core offering that app developers use to deliver services to users. It is the back-end system that developers choose to process in-app purchases (as opposed to the payment method that is selected by users – e.g., PayPal, Visa, MasterCard).
- The two major mobile platform operators mandate the use of their proprietary payment processing systems, enabling them to collect high fees of up to 30% on all in-app purchases. There are exceptions (fees reduced for businesses earning less than USD 1M on the stores; "reader apps" in Japan and apps in South Korea may use alternative processing systems on one platform) but most do not apply to games, which are the largest source of fees on the app stores.
- There is no objective justification for the conduct. One major operator did not enforce fee collection until last year, yet was able to maintain, secure, and expand its store before that time. Only 16% of apps in another store are subject to fees. Other app store operators (including Microsoft) are able to maintain secure and updated app stores without similar requirements.
- These requirements do not result in efficiencies. Third party services (such as Stripe) or developers' own services (such as Xbox) typically charge far lower fees for payment processing, which would benefit developers and their customers.

Level of fees deters adoption of alternative payment systems

- Platform operators play no role in promoting or facilitating in-app purchases.
- Commission levels undermine the model for game subscription services and advantage platform operators' own services.
- Following regulatory amendments enabling developers to add an alternative payment processing system in their apps for South Korea, the two major operators have agreed to lower the commissions charged for in-app purchases to 26% when an alternative payment system is used to process in-app payments
    - Developers need to pay two sets of fees: (i) fees associated with the alternative payment processing system and (ii) the operators' commission/service fees.
    - Thus, the still-high fees render using an alternative processing system commercially unworkable.

Alternative payment processing systems

- Microsoft’s App Store Principles allow developers to use alternative payment processing systems for in-app purchases on the Microsoft Store.
  - Developers can choose to use Microsoft’s payment processing system, a secure third-party system of their choice, or their own system.
  - Microsoft charges a commission of 12-15% to use Microsoft’s payment processing system.
- Competition within mobile ecosystems could be enhanced by addressing concerns over the level and structure of commissions/service fees.
  - App developers are best placed to decide which combination of payment processing characteristics are best for in-app purchasing in their apps.
  - Payment processors (including the payment card industry (PCI)) could offer a service/back-end that everyone could use. This could reduce the fees to under 5% (compared to the current 30%).

Mandatory use of platform operator’s browser engine

- Protecting against security and privacy threats is fundamental to browser design, and browsers compete to provide enhanced functionality without compromising security.
- Security justifications for the mandatory use of a platform operator’s own browser engine are overstated and illusory.
    - Browsers based on other engines have superior security capabilities
    - Other browsers use a ‘modular’ approach to coding that protects against security attacks by keeping the code apart until it needs to be compiled
    - Other browsers do not have code writing and executing in the same place in the app sandbox, which means that they do not need to access device CPU hardware security
    - Other browsers do not employ a ‘monoculture’ approach (under which a single security breach or malware impacts all web apps on that OS)
    - Any patches to the code require a full OS update (usually of multiple gigabytes)
- Allowing browser competition would not fundamentally change the platform operator’s browser security model.

Questions and Discussion