Consumer Welfare in the Smartphone Ecosystem

Evidence from India

September 2024

Consumer Welfare in the Smartphone Ecosystem

Evidence from India

September 2024

Koan Advisory Group is a New Delhi-based public policy consultancy. It specialises in policy and regulatory analysis in both traditional and emergent sectors and markets. For more information, please visit: www.koanadvisory.com

Authors
Tamanna Sharma and Lalantika Arvind

contactus@koanadvisory.com | www.koanadvisory.com

Table of Contents

List of Figures and Tables

Abstract

This paper examines how bundling products and services affects consumer welfare in digital markets, using smartphones as an example for such combinatorial products. Our survey of 5,177 Indian smartphone users across demographics and geography, explores their preferences focusing on devices, operating systems (OS), app stores, and web apps, considering factors such as privacy, safety, trust, ease of use and quality of service.

The survey shows a strong consumer preference for the integrated hardware and software experience of smartphones. Over 85 percent of respondents see the combination of OS, software and hardware as essential. The privacy, safety, and convenience offered by OS integration with app stores and individual apps also enhances consumer welfare. Around 93 percent of respondents expressed satisfaction with their OS due to these reasons.

India's draft Digital Competition bill (DDCB) 2024, aims to prevent anti-competitive practices in digital markets and restricts several activities such as tying, bundling and self-preferencing. The integration of hardware and software products in smartphones could also be considered equivalents to bundles, as defined under the DDCB. Our findings suggest that such restrictions could harm consumer welfare in the smartphone ecosystem. Consumers trust their smartphones and are highly satisfied with the functionality of the OS, preinstalled apps and app stores. Therefore, any changes made to this ecosystem will adversely affect consumers, with severe cybersecurity implications.

We find no need for ex ante or pre-emptive regulatory action. Instead, we recommend standardising technical best practices like regular OS updates and warnings about direct web installation risks. Future regulatory interventions must not hinder these practices, as they are vital for maintaining consumer trust and device security.

01

Introduction

This paper examines the consumer welfare dimensions of the combination of products and services in smartphones. Such combinations, that can also be thought of as bundles, are ubiquitous in the technology economy.

Some competition policy researchers view bundling as a practice that reduces competition, or anti-competitive, particularly in the digital market.[1] This perspective assumes that combinations of products and services can create market entry barriers, making it difficult for smaller firms to provide their services. This is because larger firms can use innovative combinations to leverage their dominant position in one market to create a monopoly in another.[2] This stance is now evident even in antitrust legislation of jurisdictions like the European Union (EU). On the other hand, some researchers argue that bundling generates efficiency gains and increases consumer welfare, even in digital markets.[3] This viewpoint is more consistent with economic literature on traditional markets. The debate around the potential ill-effects of a combinatorial approach to product and service provision is now taking root in India. But there is a stark absence of empirical evidence on either side to substantiate the benefits or antitrust traits of this approach.

India's draft Digital Competition bill (DDCB) 2024 could mark a shift away from the consumer welfare standard enshrined in the nodal competition law, the Competition Act, 2002. The DDCB prioritises subjective standards, such as 'fairness', 'contestability' and 'transparency'.[4] These standards form the guiding principles for the draft bill, however they are not defined and cast a wide regulatory net. For instance, since fairness is undefined, the regulator can term common commercial practices 'unfair'. In contrast, consumer welfare is a well-defined standard keeping price and quality of products as driving factors.[5] Consumer welfare also forms the guiding principle for the Competition Act, 2002.

The DDCB's regulatory parameters seek to regulate a wide array of entities and seem impractical in a complex growing and commercial technological landscape. This will undoubtedly impact a variety of digital industries. The bill also lists several ex ante restrictions on companies' operations. This includes anti-steering, tying and bundling, self-preferencing and limitations on third-party applications. Among these restrictions, those targeting bundling stand out as they potentially contradict established economic principles regarding pro-consumer practices.

The DDCB's restrictions also have implications for consumer privacy and security, crucial aspects of consumer welfare, especially in digital markets where price is not the primary consideration.[6] Therefore, we set out to study the impact of such restrictions using smartphones as a proxy since they represent a combination of products and services that are now ubiquitous.

Smartphones are the primary entry point for consumers into the digital space and close to half the Indian population (42 percent) owned one in 2023. These are complex ecosystems of high-tech hardware and software combinations, and are characterised by:

1. **The integration of device hardware and software,**
2. **pre-loaded software of the operating system (OS) and applications (apps),**
3. **the discovery of new apps facilitated by app stores.**

We aim to understand how consumer preferences are impacted when the device maker's ability to freely combine these elements is restricted.

This research explores two key hypotheses. **First, the compatibility of a smartphone with its hardware and software components is essential for consumers to derive value. This includes components such as cameras, microphones, app stores and apps. Second, the security and safety provided by integrating a smartphone OS with other common features such as app permissions, and location access, benefits consumers**.

We surveyed approximately 5,000 smartphone users across India from April to May 2024 to assess their device preference for OS, app stores, and web apps, with a focus on price and non-price factors like privacy, safety, trust, ease of use and quality of service. These factors influence user satisfaction and decision-making. Additionally, these metrics are critical to assess consumer welfare in the context of policy interventions.

The first phase of the survey, carried out on-ground spanned 10 urban and semi-urban cities (i.e., tier-I and tier-II)[8] from April to May 2024, and interviewed 3,026 respondents. The second phase conducted online, covered all 36 states and union territories, with a sample of 2,151 respondents. This strategy was designed to ensure diverse demographic representation. Moreover, the online survey targeted younger, tech-savvy smartphone users while the offline survey helped us reach older populations and inexperienced, or lesser tech-savvy users. This approach allowed us to assess varying expectations and needs of users across different demographics and socio-economic backgrounds.

For example, younger smartphone users are typically willing to pay a premium for access to the latest technologies, such as 5G compatibility and longer battery life. Given their familiarity with the latest tech, they can navigate security and update protocols . In contrast, older generations and digital migrants[9] tend to prioritise user-friendly features and affordability, often relying on built-in safety measures or assistance from family members to manage device security. Covering such diverse perspectives was also essential to inform future policy decisions that are inclusive in nature.

Our research aims to fill a gap in literature on the potential impact of ex-ante, or preemptive, competition rules in India's digital markets. We hope it provides valuable evidence for policymaking on digital markets, which often lacks sound empirical data.

Overall, our findings reveal a strong consumer preference for the integrated hardware and software experience offered by smartphones. We evaluated multiple such combinations: the fundamental integration of device hardware and application software, pre-loaded software packages of OS and apps, and the app stores that facilitate discovery of new apps. **We found no case for regulatory intervention, were these to be considered equivalent to bundles as defined under the DDCB. This finding carries significant policy implications. First, any regulatory changes impacting combinations or bundles requires thorough empirical evaluation and impact assessment. Second, the high level of trust consumers place in combinatorial products demands equal responsibility on device makers and software providers.**

Figure A: Integration of Hardware and Software in a Smartphone

Consumers also expect smartphone brands to meet high standards of security and quality of service. While mainstream brands typically meet these expectations due to intense competition in the devices market, the wider smartphone market has many differentiated brands. Therefore, the standardisation of best practices, such as regular OS updates and warnings about risks of direct web installations, are essential to maintaining consumer trust and ensuring device security and reliability. In this context, soft law measures may prove more useful from a consumer welfare and public interest standpoint. On the other hand, untested ex ante prescriptions that seek to limit prevalent commercial practices in smartphones are likely to reduce consumer surplus. This is evident from the decisive direction of our survey results as well.

The takeaways from our survey are:

Over 85 percent of respondents believe that the smartphone OS, its related software, hardware, and external peripherals are all essential value additions to their device

- Consumers derive significant value from both the hardware and software components of their smartphone. They view their phones as composite and versatile tools for communication, entertainment, productivity, and more. Smartphone manufacturers and OS providers facilitate this ecosystem by ensuring safety, security and quality of service, when providing products and services as a whole. Ex ante competition regulations that equate such combinations with the notion of bundles will negatively impact consumer welfare. Some specific trends are:
    - Of the respondents surveyed, an overwhelming majority value both hardware and software. Specifically, 87.8 percent find smartphone's OS and software important, 88.2 percent prioritise hardware features like display, RAM, battery, and camera, and 87.3 percent consider external peripherals and after-sales services essential.
    - Majority (93 percent) of the survey respondents express satisfaction with the current functioning of their OS. They agree that it effectively maintains user security and privacy. Moreover, the user interface is easy to navigate, which is particularly important for digital migrants. Consumer satisfaction is driven by factors like convenience (32.8 percent), inbuilt safety and security (32.7 percent), and ease of use (34.2 percent) of the OS.

Nearly 87 percent of respondents exercise a high-degree of agency in selecting apps, finding it easy to download their preferred choices from app stores

- Consumers seem highly satisfied with preinstalled apps. Majority (87.9 percent) are satisfied with preinstalled apps. Irrespective of the availability of preinstalled apps, consumers can easily download other apps from app stores and 86.9 percent find it easy to install apps on their device from an app store.

- Evidently, consumers exercise agency in terms of app choices. The presence of preinstalled apps, which can also be thought of as combinatorial products, is not a negative externality. Preinstalled apps typically undergo rigorous vetting and security checks. They also lower search costs for consumers to find apps that fulfil their functional needs. These apps serve as secure entry points for digital migrants unfamiliar with the download process.

Majority (89.8 percent) of respondents consider compatibility with apps an important feature of their smartphone, and 91.8 percent regularly update their phone's software, ensuring device security

- Consumers want their smartphone apps to function glitch-free and regularly update their smartphone software. Regular OS updates maintain app compatibility, and protect consumers' devices from malware, bugs, etc. For instance, if an app requires certain permissions, most smartphones' OS recognises this requirement and responds accordingly, based on the user's preferences. It protects user data from unauthorised access or exposure to malicious entities. Therefore, smartphones' functionality is optimised to suit consumers. Specifically:

    - Mainstream OSs provide a high degree of compatibility with apps, ensuring the most popular apps work seamlessly with a user's smartphone. Majority (89.8 percent) of our survey respondents consider it an essential factor. And this aids consumer welfare because compatibility of apps is inherently linked to cybersecurity.

    - Consumers regularly update their smartphones to maintain glitch-free functioning of their devices. Most (91.8 percent) regularly update their phone's software, and a mix of factors drive this behaviour - this includes maintaining app compatibility (31.5 percent), ensuring high security (34.1 percent), and receiving the latest OS features (33.7 percent). Additionally, some noted that regular updates help maintain high-speed performance.

    - Intricate technical features like the convenience of being able to restore old files and phone preferences from an old device to a new one is also very important to 85 percent of respondents.

Direct web installations and the use of multiple app stores is prevalent. More than 50 percent of our survey respondents use web installations and multiple app stores to download apps

- App installations from SMS/WhatsApp/Telegram/Third-party links, etc. and internet browsers and websites are quite prevalent. Approximately 50 percent of our survey respondents use

these external sources to download apps. About 68 percent of respondents also use multiple app stores to download apps. Preference to download apps from the preinstalled app store of the phone is slightly higher than these external sources (18 percent higher) - implying there is inherent value in the app store-OS-device combination, however, the prevalence of direct installations raises potential cybersecurity concerns.[10]

More than 70 percent of respondents rely on user-generated inputs such as ratings, reviews and number of downloads for installing apps

- App stores provide consumers with valuable metrics such as ratings, reviews, and number of downloads, that assist in their app downloading process, thereby promoting user agency. These metrics, which influence app download rates, are diverse, and users play a pivotal role in building these metrics. This includes brand credibility, the most important factor for 78 percent of consumers, followed by ratings, reviews (74.3 percent), and number of app downloads (70.2 percent). The least important factor for downloading an app is recommendation from a friend (66.5 percent). The DDCB limits restrictions on installation of third-party apps and software.[11] This could have unintended negative consequences such as the ability of OS providers to caution against unverified third-party app stores on smartphones and potentially harmful apps that may contain malware. This is because not all apps and app stores employ robust security measures. Therefore, preventing OS providers from placing security restrictions could lead to security implications.

More than 80 percent respondents agree that preinstalled app stores are essential as they facilitate the discovery of secure and tested new apps and are easy to use

- App stores contribute to consumer surplus by lowering search costs for consumers. They function as more than just hosting platforms; they offer a seamless and secure way to improve digital access at no or limited cost. More than 80 percent respondents expressed satisfaction with preinstalled app stores, as they are easy to use, making app downloading an easy task. Respondents also indicate high degrees of confidence that their app stores provide secure and tested applications.

02

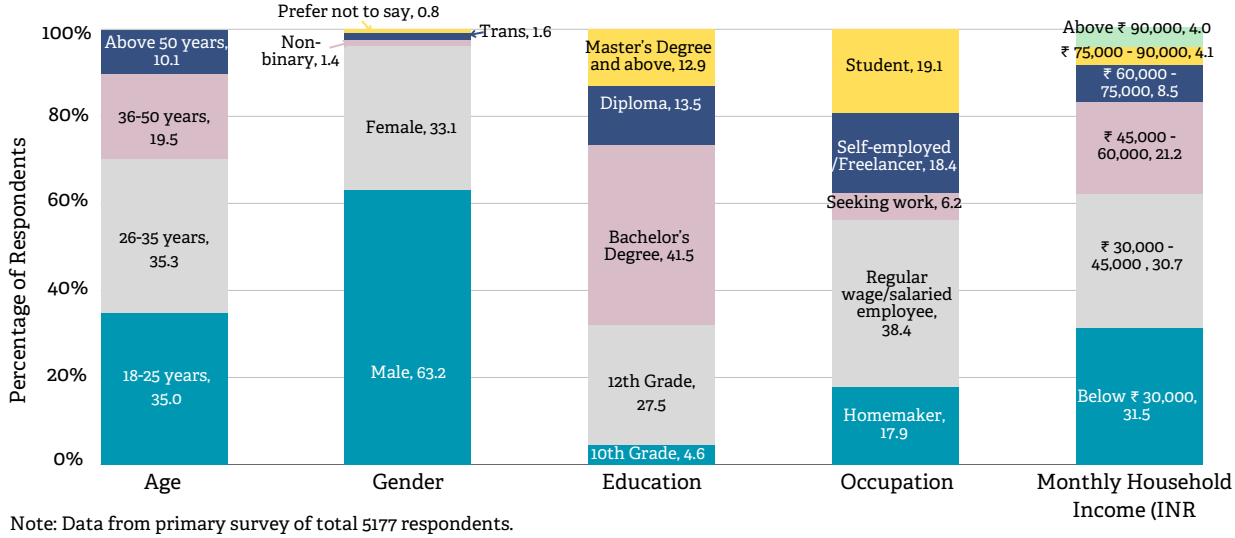
Survey Design and Respondent Profiles

We conducted a survey of 5,177 smartphone users across the country, to understand consumer preferences for integrated hardware and software products in the smartphone ecosystem. The survey was conducted in two phases to maximise reach and ensure representation from a heterogeneous demographic. The first phase was conducted on-ground, across ten urban and semi-urban cities, that is tier-I and tier-II[12] cities from April to May 2024, with a total sample of 3,026 respondents. The second phase of the consumer survey was conducted online, covering all 36 states and union territories, with a total sample of 2,151 respondents.

The online survey targeted younger, tech-savvy smartphone users, while the on-ground survey helped us reach first-time smartphone users and an older demographic. This also allowed us to cover individuals from different socioeconomic backgrounds as they tend to have varying expectations and needs from their personal devices.

On average, our survey respondents represent an educated, working-class population from diverse income groups (see Figure 1). About 63 percent of the respondents were men. Around 70 percent of all respondents were between the ages of 18 to 35 years. Nearly 68 percent of the respondents had a bachelor's degree or higher. More than half, at 52 percent, had monthly household incomes between ₹30,000 - ₹60,000. This demographic, encompassing both tech-savvy and novice users, effectively captured a broad range of expectations for smartphone features and performance.

Figure 1: Respondents Profiles



Note: Data from primary survey of total 5177 respondents.

03

Survey Results and Literature Review

We discuss the key findings from the consumer survey, analysed within the context of relevant economic literature on the impact of bundling in digital markets.

We evaluate three different types of hardware and software combinations:

1. the integration of the device and the OS;
2. pre-loaded package of OS and apps, and
3. app stores and the discovery of new apps.

Our questions focussed on consumer preferences related to these combined products, evaluating qualitative factors such as privacy, safety, trust, ease of use and quality of service, keeping price as the baseline comparative metric. These factors were selected because they significantly impact user satisfaction and decision-making. Additionally, they are critical in assessing consumer welfare in the context of policy interventions.

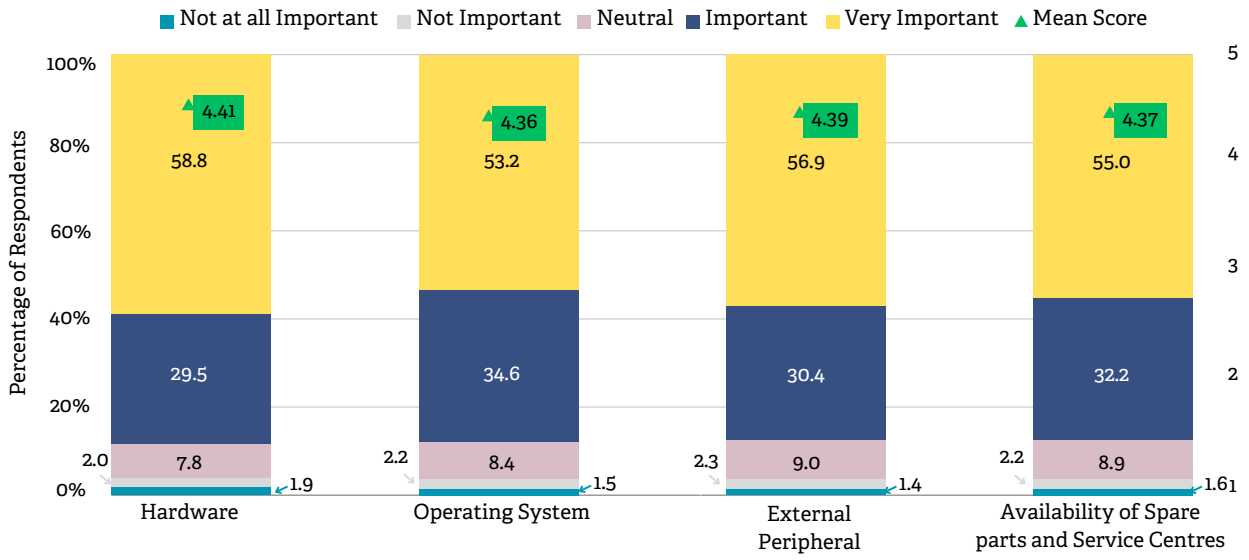
3.1 The Device and OS

At its core, the essence of a smartphone resides in its OS. An OS enables software functionalities such as data and storage management, network communication, and memory processing. It also operates and manages physical hardware components such as cameras and microphones, GPS sensors, and Bluetooth signals.[13] For consumers, these features represent distinct functional aspects of smartphones, and their utility is measured in terms of factors like responsiveness, quality and convenience. For instance, a prospective smartphone buyer might enquire about a device's data storage capacity, its camera lens, or the available runtime memory of the device. These are examples of the many factors that determine the efficacy of different apps on the device.

We asked consumers to evaluate hardware and software specifications, using cost as the relative baseline factor. We find that consumers take a composite approach where hardware functionality, OS performance, and customer support are all relevant factors informing their choice. For instance, 88.2 percent of survey respondents stated hardware features such as high-quality displays, sufficient RAM, long-lasting batteries, and other components are essential considerations. At the same time, 87.8 percent consider the OS and its software version to be important (*see Figure 2*).

External peripherals, such as additional accessories or connected devices like USB cables and charging plugs, also add to the value of a smartphone and are considered essential by 87.3 percent of our survey respondents. Additionally, after-sales services are crucial for the same share of 87.3 percent consumers (Figure 2). This includes the availability of spare parts and service centres, ensuring that any issues with the smartphone can be promptly and efficiently addressed.

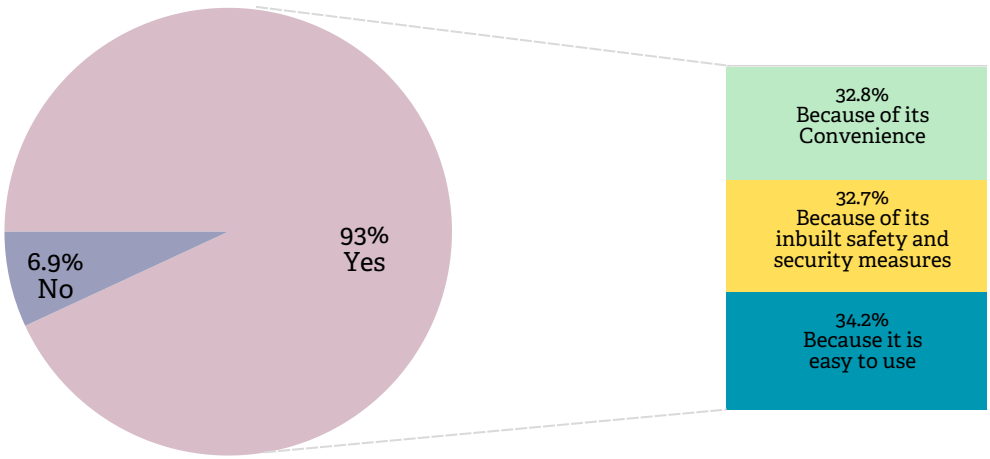
Figure 2: Important Features of a Smartphone



Note: Data from primary survey of total 5,177 respondents. Note: Respondents rated factors on a five-point Likert scale, with "Not at all Important" being 1 and "Very Important" being 5. Mean scores represent the weighted average of responses.

These results show that consumers expect end-to-end servicing and functionality from the purchase of a smartphone, which they view as a single, indivisible unit. 93 percent of respondents also showed high levels of satisfaction with the current performance of their OS. Of this, 32.7 percent of the respondents acknowledge that OSs help maintain user security and privacy, a similar share of 32.8 percent of respondents said OSs provide convenience and approximately the same number said OSs are easy to navigate (34.2 percent), which proves all three factors are equally important (*see Figure 3*). These providers maintain safety and ensure compatibility for the end-user by integrating its product with the hardware of device manufacturers, or Original Equipment Manufacturers (OEMs), and the apps developed by various developers.

Figure 3: Satisfaction with an Operating System



Note: Data from primary survey of total 5177 respondents. Survey respondents were given multiple choice options for reasons of satisfaction with the OS. Hence the total percentage of responses for those who selected "Yes" is greater than 93 percent.

There are two types of partnerships between OS providers and OEMs that determine the nature of the device and the OS integration. First, OEMs make their own proprietary OS, like Apple iOS, which is a closed-source environment.[14] Second, brands like Google license OS like Android to other OEMs.

While compatibility is implicit in the first case, when the OS is licensed to third-party OEMs, a contractual agreement typically exists to ensure compatibility. For instance, Google mandates manufacturers to meet specific baseline technical standards as a condition to licensing Google's proprietary mobile apps.[15] This ensures that compliant Android-based smartphones will be able to run Android apps properly and protect consumers' sensitive and personal information. This compatibility framework enables the OS provider to implement robust security measures in the device such as data encryption, app sandboxing, permissions management, and regular software updates.[16] These inbuilt safety protocols therefore protect consumers. They are particularly advantageous for digital migrants or the less tech savvy population, who rely on OS security protocols to provide a safe and secure environment.

However, compatibility agreements are likely to attract scrutiny under the DDCB 2024. The DDCB classifies tying, bundling, and self-preferencing as anticompetitive and restricts target enterprises from engaging in these practices. Section 11 of the DDCB prohibits large digital platforms, called Systematically Significant Digital Enterprises (SSDEs) from self-preferencing, while Section 15 of the DDCB prohibits SSDEs from bundling and/or tying any services, even those of third parties. The DDCB could view an OS provider requiring OEMs to adhere to certain security protocols and app standardisation requirements as a form of bundling.

Our findings suggest that enforcement of the DDCB will negatively impact consumers, exposing them to cybercrime, cyber fraud, software bugs, and malware risks associated with incompatible OS versions. For instance, without standardised security protocols or Application Programming Interfaces (APIs), consumers will not be able to access relevant security updates.[17] This could also expose consumers to potentially harmful apps, further risking their sensitive and personal information.

Indian app developers and OEMs would also face greater security, malware, and intellectual property misappropriation risks. The DDCB will therefore negatively impact both business users and consumers, lowering welfare for all stakeholders involved.

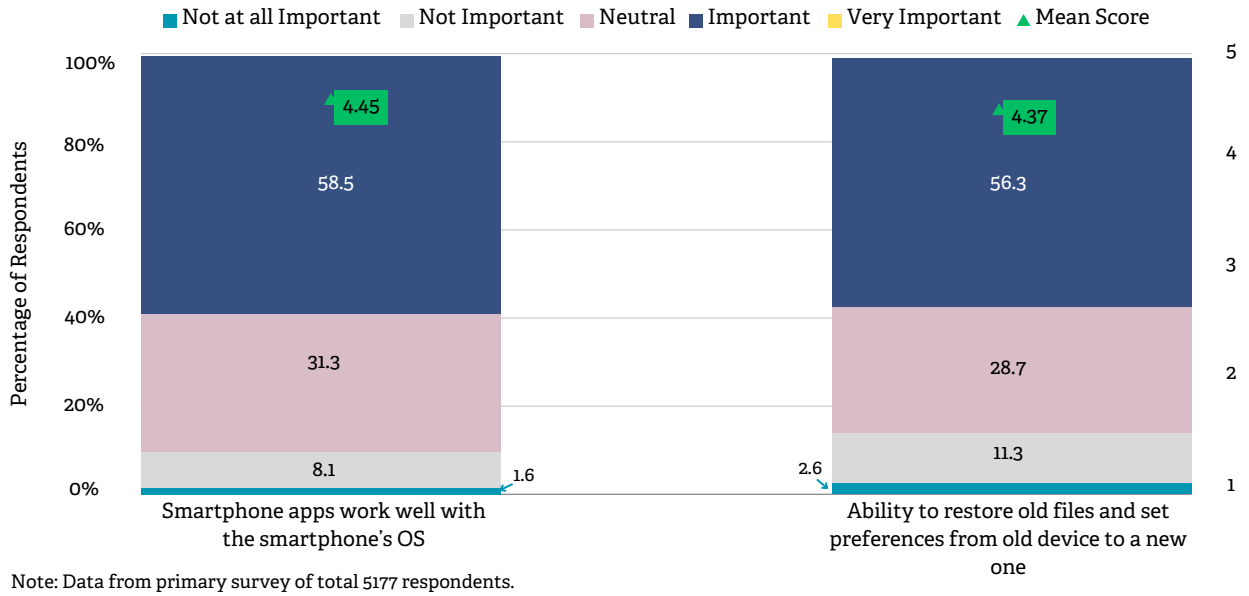
Increased security risks and fragmentation of the OS ecosystem will therefore undermine consumer trust and escalate costs, posing a threat to India's growing digital economy. Any regulatory intervention that limits OSs capability to safeguard consumers, while maintaining their product quality, must carefully consider the potential adverse effects.

3.2 Compatibility of Smartphone Apps

Maintaining compatibility is critical to ensuring that apps run properly on a specific device.[18] From a consumer standpoint, a device's compatibility is essential as it guarantees consistent app performance and eliminates the burden of ensuring cross-platform integration. At the same time, it provides a layer of protection and security to consumers' devices by only allowing the installation of apps that have undergone rigorous security checks and are built on standardised APIs. For instance, apps that are not vetted by preinstalled app stores are allowed on Android devices, but users are generally cautioned about such installations since they could contain harmful content or malware.[19] Closed ecosystems such as the Apple iOS, generally do not allow third-party app installations outside of their app store.[20]

Our survey results also show that consumers deeply care about the functionality of apps on their smartphones. 89.8 percent agreed that OSs provide a high degree of compatibility with smartphone apps, ensuring most popular apps work seamlessly with a user's smartphone (*see Figure 4*). And this aids consumer welfare because compatibility of apps is inherently linked to cybersecurity.

Figure 4: Convenience offered by an Operating System



Note: Data from primary survey of total 5177 respondents.

App compatibility is achieved by device manufacturers committing to follow baseline compatibility requirements. For example, open-source OS providers like Google implement compatibility measures through compatibility agreements on devices that carry proprietary applications licensed under an app licensing agreement such as Mobile Application Distribution Agreement (MADA).[21] Such agreements enable OEMs to license proprietary elements like app APIs and preinstall desired apps. OS providers' APIs also allow developers to integrate functionalities like push notifications, location services, and security features, enhancing app quality and user satisfaction.[22] Licensing these services together also ensures that faulty APIs are identified at the manufacturing stage, mitigating risks of data breaches and preventing apps from malfunctioning.[23] In the case of closed ecosystems such as the Apple iOS, app compatibility is ensured by preventing any third-party modification of the OS.[24]

The DDCB would thus make it difficult for OS providers to enforce compatibility through license agreements and negatively impact consumer welfare. The responsibility of ensuring that apps work well with smartphones will then fall directly on consumers, significantly increasing their time and search costs. Moreover, altered APIs may increase security risks for consumers. Consequently, this will also lead to an increase in operational expenses for developers, as consumers would turn to them for assistance with issues in app functionality. Developers would also be forced to devote resources to redesign their apps to address the inconsistent API frameworks across devices

Regular OS updates are another crucial aspect for maintaining device security and compatibility, which is enabled by standardisation of APIs.[25] This is an essential aspect for consumers, who want glitch-free functioning of their apps and are generally diligent with updating their smartphone's software.

Neglecting updates can also expose consumers to security risks, limiting the OS and app store's ability to detect and address potential threats[26] – a factor that consumers seem to be aware of. Our survey results indicate a high user compliance rate (91.8 percent) with software updates, driven by priorities such as app compatibility (31.5 percent), enhanced security (34.1 percent), access to new OS features (33.7 percent), and improved device performance (*see Figure 5 and Figure 6*). Advanced OS features like seamless data migration from old to new devices - valued by 85 percent of the survey respondents, further exemplify the functionality offered by an OS (*see Figure 4*). Therefore, ensuring compatibility of the OS with the device is essential to build consumer trust and provide a uniform experience to the user.

Figure 5: Do consumers regularly update smartphones?

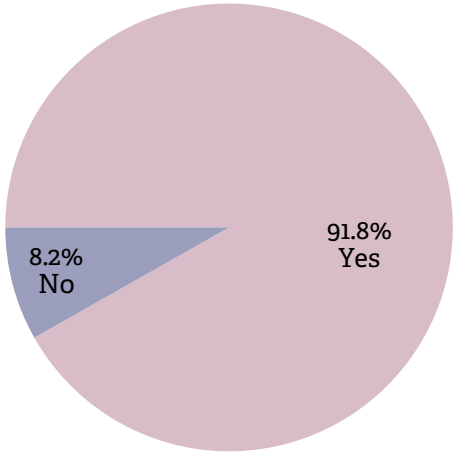
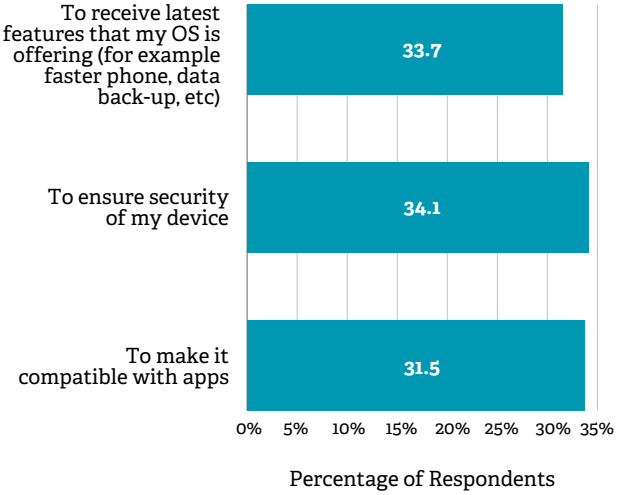


Figure 6: Reasons for Updating Smartphone



3.3 Preinstalled Apps, OS and Smartphones

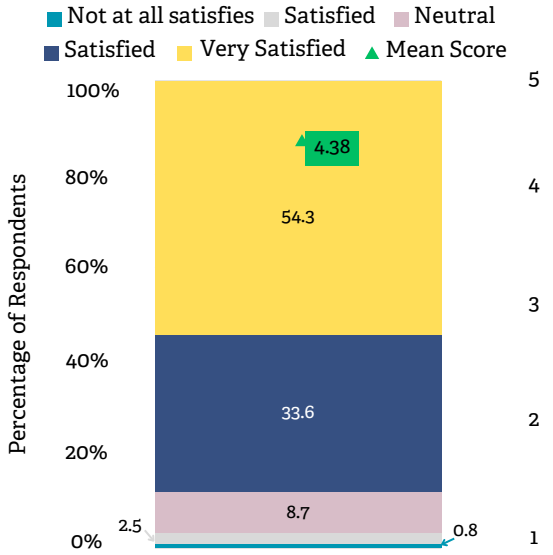
A second layer of product integration in the smartphone ecosystem involves the OS and preinstalled apps. Open-source software allows OEMs to offer custom versions of the OS. For instance, Android OEMs can separately license a set of proprietary preinstalled apps. Most smartphone manufacturers leverage this capability to differentiate their products in the market, often through partnerships with mobile network operators (MNOs), social networks, and content providers.[27] These partnerships enhance the appeal of smartphones, making preinstalled apps an asset for OEMs.

However, some regulators view the preinstallation of apps as potentially anticompetitive. The first concern is that preinstalled apps may pose privacy risks, making consumers' data more vulnerable. The second argument is that preinstallation constitutes a form of self-preferencing, restricting consumer choice and information.[28] Under the DDCB, preinstalled apps could face scrutiny due to restrictions on self-preferencing. This regulatory shift could signal the end of preinstalled apps, fundamentally changing the landscape of smartphone software provisioning.

Despite occasional calls for greater regulatory scrutiny, largely based on anecdotal evidence, our survey found that an overwhelming majority of respondents (at 87.9 percent), are satisfied with preinstalled apps. Additionally, consumers can easily download other applications from app stores,

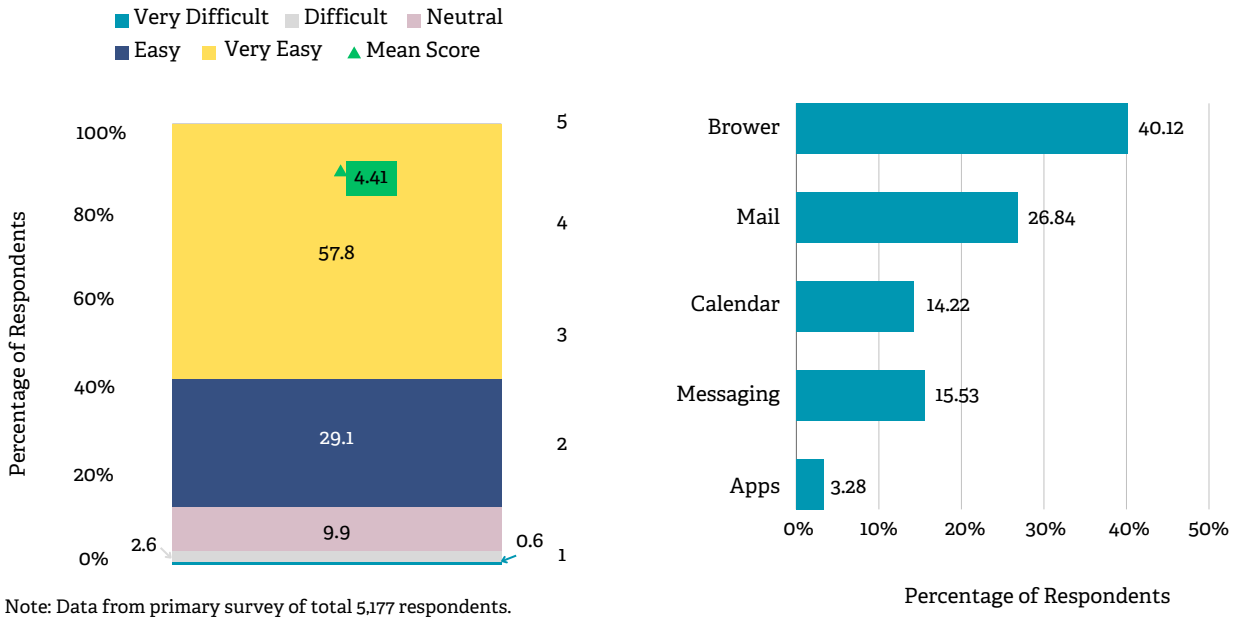
with 86.9 percent finding it easy to install apps on their devices. This demonstrates that users exercise agency in selecting and managing their apps. According to our survey, browsers (40.1 percent), mailing apps (26.8 percent), and messaging apps (15.5 percent) are the top three categories of apps downloaded by users, which are also prominent categories for preinstalled apps (*see Figure 7 and Figure 8*).

Figure 7: Satisfaction with Preinstalled Apps



Note: Data from primary survey of total 5,177 respondents.

Figure 8: Ease of Installing Apps and Types of Apps Installed



Note: Data from primary survey of total 5,177 respondents.

The presence of preinstalled apps, which can also be thought of as combinatorial products, is not a negative externality for consumers. In fact, preinstalled apps lower search costs by providing ready-to-use solutions that meet their functional needs. Such functionality is particularly valuable for digital migrants, who may be less familiar with the app downloading process. These users are likely to rely on OEMs to provide safety-by-design, and user-friendly platforms as their initial touchpoints, making preinstalled apps an important feature of the smartphone. This is particularly important in the Indian context, where more than 50 percent of the country's population[29] is yet to be connected to a smartphone. Research supports the legitimacy of such practices provided they enhance consumer choice, and reduce distribution and search costs.[30] Preinstalled apps typically undergo rigorous vetting and security checks, making it safe for consumers to use.[31]

Overall, our findings suggest that there is no case for regulatory intervention for preinstalled apps. However, it is important to acknowledge documented cases of preinstalled apps posing security vulnerabilities, as in the case of certain Chinese smartphone brands.[32] This highlights the need for heightened cybersecurity vigilance, particularly in safeguarding the ability of operating systems to secure devices.

3.4 The App Store and OS

Integration of the OS and app stores play a pivotal role in enhancing consumer welfare by streamlining the process of app discovery and installation, significantly reducing search costs and improving access to various digital services.

Results from our survey show consumers generally express high confidence in the preinstalled app stores of their phones, attributing this trust to factors like an easy user interface (85.5 percent), rigorous security measures and scanning protocols (83.5 percent), the availability of popular and preferred apps (80.8 percent) and the convenience of having a preinstalled app store on their device (80.4 percent) (*see Figure 9*).

Among these features, the security and safety of downloading apps remains a central point of contention for app store regulation. For instance, the European Union's Digital Markets Act (DMA) aims to increase competition in the app store ecosystem by allowing alternative or third-party app stores to operate on devices. Article 6(4) of the DMA requires OS providers to allow consumers to directly download apps from external sources and not place any restrictions on third-party app stores. However, OS providers do have the right to impose restrictions on such downloads if they are necessary, proportionate and duly justified, especially to secure the device.

Proponents of allowing users to install third-party app stores, as available on open OS ecosystems, argue that it would foster innovation and offer consumers more choices, potentially lowering costs associated with app purchases.[33] The DDCB mirrors the EU's DMA, limiting restrictions on third-party apps and direct web installations. Section 13 of the draft bill mandates that an SSDE shall not restrict or impede the ability of end users or business users to download, install, operate or use third-party applications or other software on its Core Digital Services. The EU however allows restrictions on such downloads if it is necessary for security concerns.

For instance, Android's practice of cautioning users about the risks of direct web installations serves as a necessary security measure. The DDCB could prevent OS providers from implementing such measures, even if they are necessary for security reasons.

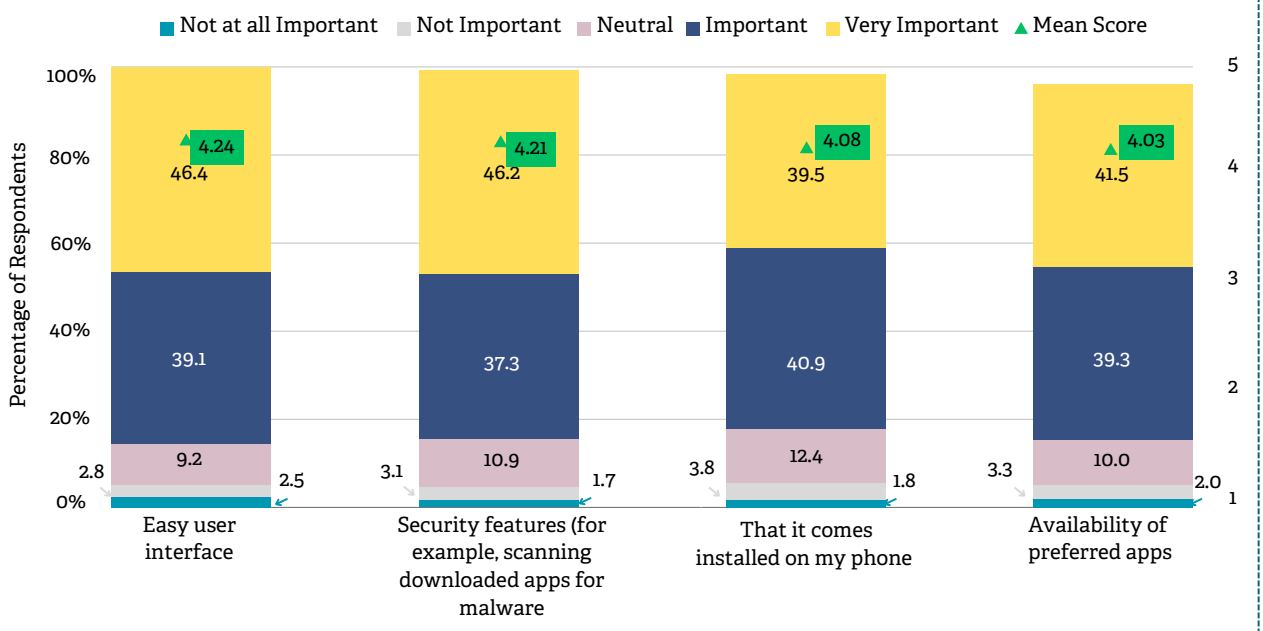
A proliferation of unverified, user-installed, third-party app stores potentially increases security risks.[34] Third-party app stores installed by users and external sources of app downloads pose inherent risks to consumer welfare. This is because such alternative platforms may lack the stringent security measures implemented by preinstalled app stores or those developed by the OS or OEM. For instance, third party app stores installed by users are the leading cause of malware on Android, according to a 2021 Nokia Intelligence report.[35]

Consumers generally prefer OS developers' preinstalled app stores due to the assurance of security features. For instance, on Android, Google Play Protect actively scans for and removes potentially harmful apps to protect user data.[36]

Despite a preference for downloading apps from preinstalled app stores, consumers use additional app stores of their choice. Our survey shows that 68.9 percent of consumers use multiple app stores to download apps.[37]

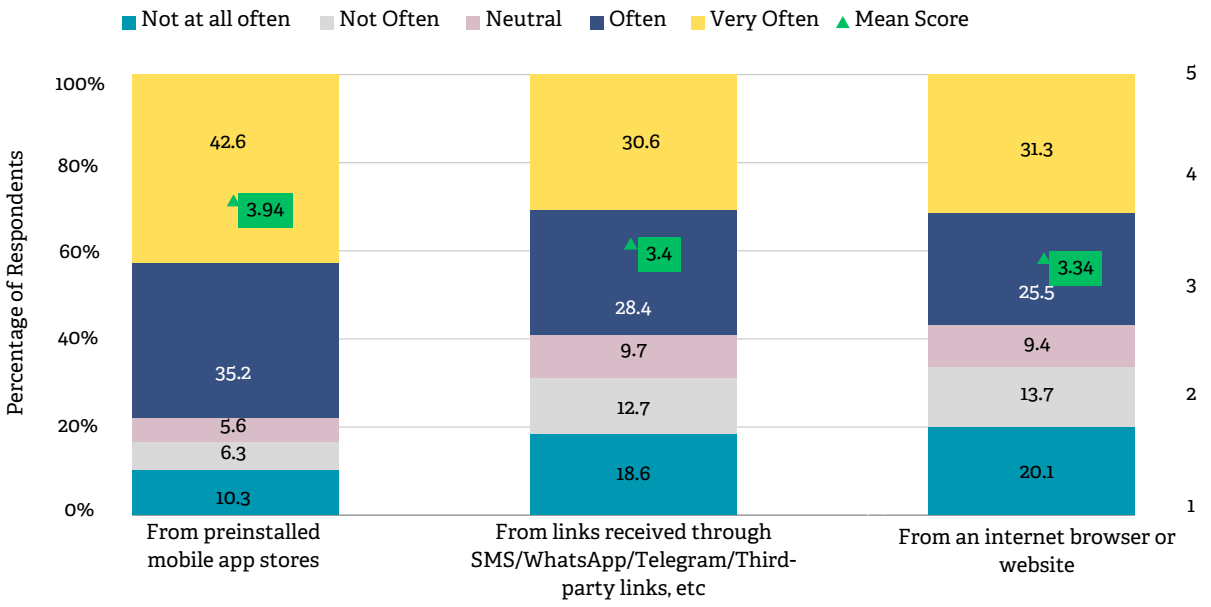
This finding aligns with our survey results where 86.9 percent of respondents indicated that they find installing apps to be an easy task (*see Figure 8*). App downloads from app stores are 18 percent higher compared to internet browsers or websites, which is the least used method for downloading apps. Further, direct web installations are also prevalent. App downloads from SMS/WhatsApp/Telegram/third-party links, which are roughly comparable to internet browsers or websites, are generally high. Approximately 50 percent of our survey respondents use such external sources to download apps (*see Figure 10*). Such a prevalence of direct web installations is a potential cybersecurity concern. Regulatory intervention should focus on increasing consumer awareness about the potential ill effects of accessing apps through unverified or external sources. The prevalence of direct web installations also indicates the importance of OS security features like cautioning against risks of such installations.

Figure 9: Benefits of an App Store



Note: Data from primary survey of total 5,177 respondents.

Figure 10: Approaches to App Installation



Note: Data from primary survey of total 5,177 respondents.

3.5 Factors Influencing App Downloads

The utility of an app store stems from two key factors:

1. its ability to aggregate various applications onto a single platform, simplifying the search for relevant apps, and
2. its inherent safety and security features, such as automatic scanning for harmful applications.[38]

Users also rely on an app's rating - an aggregate of downloads, reviews, and user feedback - as an indicator of its safety. Users rely more heavily on the security and credibility of ratings provided by preinstalled app stores, underscoring their importance in the smartphone. Our survey results reflect the same. 78.6 percent of the survey respondents indicated that the most significant factor while downloading apps is brand credibility, which is influenced by a preinstalled app store, followed by ratings and reviews (74.3 percent), and the number of app downloads (70.3 percent). The least important factor is peer recommendations (66.5 percent) (*See Figure 11*).

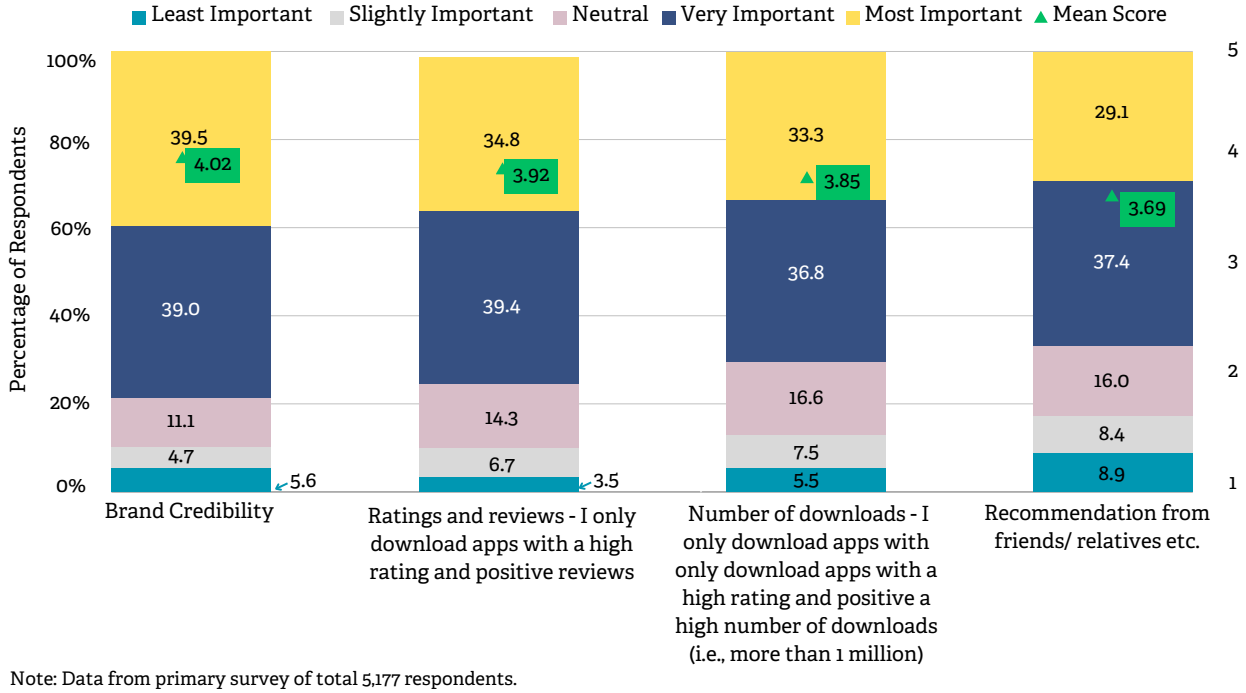
Restrictions on limiting third-party app stores, as outlined in the DDCB, overlook the importance consumers place on user-generated information. Section 13 of the DDCB limits large digital platforms from restricting the ability of end users and business users to download, install, operate or use third-party applications or other software.

Third-party app stores installed by users or other external sources may not offer the same level of security that preinstalled app stores would. This can hinder consumers' ability to identify potentially harmful apps, thus lowering consumer welfare.

Closed platforms like iOS generally do not encounter the issue of harmful web apps as their ecosystem does not permit direct web installations. However, most open-source OS providers display warnings or declaimers during direct web installations, a standard practice that protects users from potentially harmful apps. The National Company Law Appellate Tribunal (NCLAT) also emphasised that such disclaimers are an essential security obligation under Indian Information Technology laws.[39]

Section 13 of the DDCB by limiting the ability of large digital platforms to restrict third party app stores, could potentially imply that disclaimers for direct web installations are also blocked. This has the potential to negatively impact consumers and heighten their security risks.

Figure 11: Factors Impacting App Downloads



Note: Data from primary survey of total 5,177 respondents.

Conclusion

Smartphones generate significant value for consumers in India's diverse digital market comprising millions of digital natives and migrants alike. We surveyed 5,177 users to assess consumer preferences across three hardware and software combinations in the smartphone ecosystem - (a) the integration of device hardware and software, (b) pre-loaded software packages of the OS and apps, and (c) app stores and the discovery of new apps.

Seamless integration between hardware and software is fundamental to smartphones and enables collaboration between OS providers, OEMs and app developers for compatibility across device features and apps. This synergy is highly beneficial for consumers, who view their smartphones as a single, indivisible unit, equally valuing hardware functionality, OS performance, and support services. OS providers ensure compatibility and functional integration through licensing agreements that mandate manufacturers to implement standardised security protocols and use standardised APIs. These protocols enable the deployment of robust security measures such as data encryption and permissions management, protecting devices against potential threats and enhancing consumer confidence in the device's safety. Such measures also ensure a consistent and standardised app experience, significantly boosting consumer welfare. The proposed ex ante restrictions on tying, bundling, and self-preferencing, as outlined in the DDCB, pose a threat to the existing security protocols and app standardisation of OS providers. These restrictions, which could potentially view hardware and software integration of the smartphone as a bundle, may expose consumers to cybercrime, bugs, and malware, and disrupt their app experience due to incompatible OS apps. This will inadvertently lower consumer welfare.

At the second level, ex ante rules that restrict an OS' ability to preinstall apps negatively impacts consumer welfare. Apps on preinstalled app stores generally undergo rigorous vetting procedures and must meet strict security standards. This process instills high confidence in consumers regarding the security and reliability of the apps available on OS providers' preinstalled app stores. Additionally, app stores enhance consumer welfare by imposing appropriate security and compatibility requirements on developers. They also reduce search costs for consumers by acting as aggregators, fostering a trusted network between consumers and developers. This approach ensures that developers have stable distribution costs, and ensures product quality, further enhancing consumer welfare.

Preinstalled app stores also facilitate the discovery of new apps in a safe ecosystem thereby enhancing consumer choice by aggregating relevant information in a single platform. This functionality is an integral benefit when the smartphone is viewed as a bundle, since it allows consumers to identify potentially harmful apps.

Across all layers of the smartphone ecosystem, consumers explicitly prefer the benefits of combining hardware and software elements and enjoy access to their preferred apps. The ex ante restrictions proposed within the DDCB could disrupt prevalent commercial product combinations, perceived as bundles, in the smartphone market. This is likely to negatively implicate consumer welfare and cybersecurity in India's smartphone ecosystem, impacting all market participants, including consumers, app developers, and OEMs. We therefore recommend policymakers undertake similar empirical studies to understand market dynamics before effectuating any such changes.

Endnotes

1 Edelman, 'Does Google leverage market power through tying and bundling', Journal of Competition Law & Economics 11, no.2 (June 2015), pp 365-400; Q. Wu & N. Philipsen, 'The Law & Economics of Tying in Digital Platforms: Comparing Tencent and Android', Oxford Journal of Competition Law & Economics (2023)

2 Qian Wu and Niels J Philipsen, "The Law and Economics of Tying in Digital Platforms: Comparing Tencent and Android," *Journal of Competition Law & Economics* 19, no. 1 (March 1, 2023): 103–22, https://doi.org/10.1093/joclec/nhac011.

3 Nicholas Economides and Ioannis Lianos, "The Elusive Antitrust Standard on Bundling in Europe and in the United States in the Aftermath of the Microsoft Cases," SSRN Scholarly Paper (Rochester, NY, November 11, 2009), https://papers.ssrn.com/abstract=1078932.
D. Mandrescu, 'Tying and bundling by online platforms- distinguishing between lawful expansion strategies and anti-competitive practices', *Computer Law & Security Review* 40 (2021) 105499:

4 The United Nations Guidelines for Consumer Protection, 1985.

5 Robert. H. Bork, The Antitrust Paradox: A Policy at War with Itself 66 97 (1978)

6 Ohlhausen, Maureen, and Alexander P Okuliar. "Competition, Consumer Protection, and the Right (Approach) to Privacy." Antitrust Law Journal 80 (2015): 134.

7 Based on a population estimate of 1.4 billion and 600 million smartphone users. Anand, S. (Nov, 2022). India has over 1.2 bn mobile phone users: I&B Ministry. LiveMint.

8 The ten cities covered in the offline survey included Ahmedabad, Bangalore, Bhopal, Chennai, Delhi, Hyderabad, Jaipur, Lucknow, Mumbai and Patna.

9 We use this phrase to describe technology non-natives or those who are new to technology and smartphones.

10 Rachel Barton (2023). How To Keep Your Business Secure When Sharing Data With Third-Party Applications. *United States Chamber of Commerce.*

11 Section 13 Draft Digital Competition Bill (DDCB) "13. Restricting third-party applications The Systemically Significant Digital Enterprise shall: (a) not restrict or impede the ability of end users and business users to download, install, operate or use third-party applications or other software on its Core Digital Services; and (b) allow end users and business users to choose, set and change default settings."

12 The ten cities covered in the offline survey included Ahmedabad, Bangalore, Bhopal, Chennai, Delhi, Hyderabad, Jaipur, Lucknow, Mumbai and Patna.

13 Geeksforgeeks (n.d.). "What is a Mobile Operating System"

14 Lukasz Grzybowski and Ambre Nicolle, "Estimating Consumer Inertia in Repeated Choices of Smartphones*," *The Journal of Industrial Economics* 69, no. 1 (2021): 33–82, https://doi.org/10.1111/joie.12239.

15 Android Compatibility Program Overview; Competition and Markets Authority (Gov.uk, n.d.)

16 Karnal Singh and Lalantika Arvind. Mobile Security - An Assessment of Cyber Security Threats in the Indian Ecosystem. November 2023, Esya Centre.

17 Ibid. Singh and Arvind (2023).

18 "App Compatibility in Android | Platform," Android Developers, accessed June 27, 2024, https://developer.android.com/guide/app-compatibility.

19 "Developer Guidance for Google Play Protect Warnings," Google for Developers, accessed July 1, 2024, https://developers.google.com/android/play-protect/warning-dev-guidance.

20 https://developer.apple.com/support/dma-and-apps-in-the-eu/#ios-app-eu

21 Competition & Markets Authority (n.d.). "Appendix E: Google's agreements with device manufacturers and app developers"

22 Ibid. CMA (n.d.)

23 "On Android Compatibility," *Android Developers Blog* (blog), accessed June 27, 2024, https://android-developers.googleblog.com/2010/05/on-android-compatibility.html.

24 "Overview of Publishing Your App on the App Store - Manage Your App's Availability - App Store Connect - Help - Apple Developer," accessed July 1, 2024, https://developer.apple.com/help/app-store-connect/manage-your-apps-availability/overview-of-publishing-your-app-on-the-app-store.

25 "Device Compatibility Overview," Android Developers, accessed July 20, 2024, https://developer.android.com/guide/practices/compatibility.

26 "Potentially Harmful Applications (PHAs) | Play Protect | Google for Developers," accessed June 27, 2024, https://developers.google.com/android/play-protect/potentially-harmful-applications.

27 Julien Gamba et al., "An Analysis of Pre-Installed Android Software," in *2020 IEEE Symposium on Security and Privacy (SP)* (2020 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA: IEEE, 2020), 1039–55, https://doi.org/10.1109/SP40000.2020.00013.

28 LiveLaw (2020)

29 Based on a total population estimate of 1.44 billion. PTI (2024). India's Population Estimated At 1.44 billion, 24 percent in 0-14 Age Bracket: UN Report. NDTV.com; Anand, S. (Nov, 2022).

30 David W. Hull, "Tying: A Transatlantic Perspective," accessed June 27, 2024, https://ideas.repec.org/h/elg/eechap/3692_9.html. Daniel Mandrescu, "Tying and Bundling by Online Platforms – Distinguishing between Lawful Expansion Strategies and Anti-Competitive Practices," *Computer Law & Security Review* 40 (April 1, 2021): 105499, https://doi.org/10.1016/j.clsr.2020.105499.

31 "Play Protect | Google for Developers," accessed June 27, 2024, https://developers.google.com/android/play-protect; see also "About App Store Security," Apple Support, accessed June 27, 2024, https://support.apple.com/en-om/guide/security/secb8f887a15/web..

32 Sarvesh M, "Indian Govt Denies Plans of Crackdown on Pre-Installed Apps," Medianama, March 15, 2023, https://www.medianama.com/2023/03/223-india-denies-smartphone-security-testing/.

33 Scott Morton and Fiona, "Entry and Competition in Mobile App Stores," 2024.

34 Bertin Martens, "Has the Digital Markets Act Got It Wrong on App Stores?," accessed June 27, 2024, https://www.bruegel.org/blog-post/has-digital-markets-act-got-it-wrong-app-stores.

35 Nokia (2021). Threat Intelligence Report.

36 "Play Protect | Google for Developers," accessed June 27, 2024, https://developers.google.com/android/play-protect; see also "About App Store Security," Apple Support, accessed June 27, 2024, https://support.apple.com/en-om/guide/security/secb8f887a15/web.

37 The question on using multiple app stores was added in the second phase of the survey, where 1,482 respondents, out of 2,151 indicated that they use multiple app stores.

38 Google Support (n.d.)

39 Ibid. Singh and Arvind (2023).

contactus@koanadvisory.com | www.koanadvisory.com