Apple's approach to protecting iPhone users, their data, and their devices, and how it is impacted by the DMA

August 2021

A smartphone is, at its core, a communications device. Apps enhance and extend the user's experience in ways that drive innovation, creativity, economic growth, and job creation. But every third party app contains code that — whether because of bugs or ill-intention — could collect and use sensitive data without consent; could alter data, hold it hostage for ransom, or leak it to the world; could engage in deceptive or fraudulent activity; or could operate in ways that disrupt the user experience or compromise the functionality of the device.

Consumers cannot see inside the apps that they want to download. Consumers who choose to buy an iPhone are relying on Apple to prevent apps from violating their privacy, their children's privacy, and the security of their most sensitive data — including private communications, location, photos, financial, and health information. They are relying on Apple to block apps that contain harmful content or fraudulent offers. And they are relying on Apple to ensure that third party apps do not interfere with their use of the phone, including by running down their battery, interfering with other apps running on the device, or compromising their ability to communicate in emergency situations.

Governments have adopted laws that similarly look to platforms to take responsibility for the content that they distribute. The DSA and similar legislative initiatives underway worldwide are intended to strengthen those requirements.

Apple is widely recognized as providing a best-in-class, 2-layered approach to managing this responsibility. *First*, it designs iOS to require that apps have user and/or Apple permission to access sensitive services, data, or technologies on the device. *Second*, it requires that all apps be downloaded from a centralized distribution system, the App Store, so that (a) human App Reviewers can confirm they are not misrepresenting or misusing these permissions, not using unauthorized permissions, and not otherwise distributing harmful/illegal content or engaging in fraudulent activity, and (b) Apple can remove apps that impermissibly change their behavior after App Review, and thereby prevent their further distribution on iOS devices. This 2-layered approach is described in further detail below.

The DMA proposes to defeat both layers of this architecture. Article 6.1(f) requires that Apple allow apps to access/interoperate with high-sensitivity aspects of the operating system, hardware, and software, in a way that opens a pathway to circumvent the technical permissions regime. Article 6.1(c) requires that Apple allow downloads from sources other than the App Store, which opens a pathway to circumvent high standards App Store rules that require transparency and prohibit harmful activity. Third party apps (including those located offshore) could also use that side pathway to circumvent government efforts to enforce local law through lawful take-down orders. And while the Commission's DMA proposal would require Apple to allow third-party app stores to distribute apps to iOS devices, its DSA proposal would not even hold them to the full baseline set of risk-mitigation obligations for "very large online platforms". In short, these elements of the Commission's proposal would significantly increase the risk to consumer privacy, security, online safety, and device health.

Governments and independent experts consistently recognize that Apple's approach provides the best protection in the marketplace for the most customers. It is hard to stay ahead of bad actors in the digital space, and Apple is constantly working to improve its protections, including for individuals that are subject to sophisticated, tailored, state-sponsored attacks. The DMA, however, would tie Apple's legs in the race to protect consumers. At a moment when consumers are asking Apple to do even more to protect them, the DMA eliminates a level of protection that Apple already has in place to manage risks from third party apps.

I. Apple mitigates the privacy, security, safety, and device health risks from third party apps by deploying a solution that combines technical protections and centralized distribution

A. iOS is designed to require that apps have permission to access sensitive device services, technologies, and data.

When an app is installed on an iPhone, it is put in a "sandbox" — in essence, a unique home directory for its files. If an app wants to access other services, data, or technologies on the device, it must have code-based permission to do so.

There are 3 types of permissions that apps can utilize:

- Apps may give themselves permission to access certain low-risk services and technologies as needed. Examples of these "self-add" permissions include the ability to store documents in iCloud and the permission to provide user names and passwords for AutoFill.
- Apps may request that a user give permission to access certain sensitive resources such as photos, contacts, and location data. The operating system requires that the app inform the user how it will use that data and that the user provide explicit consent before that access is enabled.
- Apps may request a permission from Apple to access certain services and technologies for which misuse or abuse would create a more significant risk for the user — in terms of privacy, data security, or device performance. This additional step enables Apple to ensure that the developer is a responsible entity for these sensitive entitlements or that it has the capability to implement them properly at the technical level. Examples of "managed" permissions include access to COVID exposure notification capabilities, and use of the camera while running alongside other foreground apps.[1]

Third party apps are not permitted to access directly certain extremely security-sensitive functions that Apple services use in a limited fashion to provide core functionality for users. These limitations are put in place because of the high risk that misuse or malicious use of these services or technologies could cause very significant harm to a users' data and device. For example:

- Direct access to the hard drive: iCloud Backup can both read and write to the entire hard drive of a device in order to enable data recovery from an earlier back-up. If this permission were open to third party apps, however, it could be used to encrypt and ransom all of the user's data.
- Remote erasing a device: FindMy has the capability to remotely lock and fully-erase an Apple device when it is lost. If this permission were open to third party apps, a vulnerability in either the third-party app or its server could allow malicious actors to ransom or remotely mass-erase devices.[2] Moreover, Apple would not be able to verify that the remote signal from the third-party to wipe the device is valid and actually came from the owner of that device.
- Background processing: iOS tightly manages background processing for all apps to protect battery life and processor performance. Apple applications that are built into the OS inherently have direct access to background processing capabilities, but Apple carefully writes and revises its own application code to minimize the impact on battery life and processor performance. Apple cannot scale that specialized sort of code review to millions of third party apps, nor rewrite the code of all those apps to ensure the most efficient use of background processing. Thus, if this entitlement were open to third party apps, Apple would have no way to stop an aggressive app from crowding out other apps or running down battery life. The impact would be felt by the user and every other developer whose app is trying to run on that device.

Yet even where Apple restricts permission to access certain highly sensitive services or technologies, it still works to enable equivalent functionality for third party apps in a manner that limits the risk to data security or device integrity. For example, although direct, unfettered access to background processing capabilities are limited as described above, third party apps can "self-add" entitlements to use programming interfaces that enable them to run background processing to achieve needed functionality for quick tasks (e.g., fetching email), longer running background tasks (e.g., machine learning tasks), and background processing initiated from a server based notification (a push notification). Additionally, VOIP, messaging, and location sharing apps can apply for a managed public entitlement that allows for additional background processing that supports end-to-end encrypted messengers.

Finally, there are situations in which Apple waits to open up public permission until it has tested a new technology on its own services. For example, when Apple first deployed "Hey Siri", it was only available for a very limited set of Apple's first party applications. As our engineers have grown more comfortable with the security and functionality of the feature, we have been opening up permission for more of our own applications and third party applications. This protocol enables Apple's engineers to work through the inevitable bugs or other performance issues in a context where they can see the whole picture. It also avoids a situation in which code revisions would have the effect of breaking all the third party apps that had started to use the permission. Such broad instability would be a terrible experience and significant risk for both users and third party developers.

B. *Centralized App Store distribution is designed to enable Apple to review apps to determine if they are using unauthorized technical permissions or otherwise violating App Store rules, and to remove apps from distribution if they impermissibly change behavior after review.*

The technical restrictions described above are a vital first layer of protection, but the technology alone cannot sufficiently mitigate all of the third party app risk. The operating system cannot tell if third party apps are misusing or abusing a technical permission, or making false representations to users about the services and data that they are seeking permission to access. Additionally, it cannot see if apps are engaging in fraud or distributing illegal content, and it cannot confirm that apps are abiding by heightened requirements for the protection of children.

Thus, Apple supplements OS-based restrictions with App Store rules, human App Review, and centralized App Store distribution. An app can only be distributed to iOS devices if it has been reviewed and approved by a human App Reviewer to confirm that it is using permissions appropriately and otherwise abiding by the high-standards App Store rules intended to protect our customers, including children. And because the App Store is the only distribution channel, Apple is able to effectively remove an app from distribution to iOS devices if it impermissibly changes its behavior after App Review.

This additional layer of protection reinforces the OS-based permissions regime, enforces compliance with local law, and drives ever-higher levels of privacy and consumer protection across the third party app ecosystem. For example, all iOS apps must provide for App Tracking Transparency, which requires apps to receive permission to track users across other apps. Al iOS apps must also provide for Parental Controls "Ask to Buy" settings, which allow parents to monitor their children's app-related purchases. And iOS apps may not engage in deceptive subscription practices, e.g., an app that offers a 3-day free trial that automatically turns into an expensive, automatically-renewing subscription.

II. The EC's DMA proposal disables Apple's best-in-class consumer protection architecture

As described above, Apple deploys a 2-layer architecture to protect iOS device users — one layer based on code, and a second layer based on centralized distribution that enables human review and curation of the apps that can be distributed to iOS users.

This approach significantly limits the risk that third party code will compromise user privacy, data security, online safety, and device integrity. Public authorities such as the German Federal Authority for Information Security (BSI); the EU Agency for Cybersecurity (ENISA) and the US Department for Homeland Security (DHS) agree that the best security is provided by a system without a side door.[3] DHS has recognized that centralized distribution provides "significant protection" to users.[4] Independent security experts affirm that our solution works better than others in the market place to protect the most amount of people from most attacks.[5] Consumer advocates have similarly recognized the value of requiring apps to respect high levels of privacy and consumer protection.[6]

The EC's DMA proposal opens up a pathway to circumvent this best-in-class architecture and ability to drive high privacy and online safety requirements across the app ecosystem.

- If an app can directly access/interoperate with the most sensitive device services, data, and technologies (Art. 6.1(f)), it can duck under the OS-based permissions regime designed to limit the risk to data security, privacy, and device functionality.
- If an app can be side loaded (Art. 6.1(c)), it can avoid the App Store rules and enforcement designed to prevent distribution of apps that are misusing or abusing technical permissions, or otherwise violating App Store rules intended to protect privacy, online safety, and intellectual property.

At a moment of increased consumer and citizen demand to enhance further privacy, security and online safety, the EC's DMA proposal would weaken the protections that Apple currently has in place.

III. The DMA should leave space for market solutions that are intended to protect consumers while still enabling fair competition

Regulation needs to take account of the real and present dangers from millions of lines of third party code that can be inefficient, buggy, surreptitious, or malicious and ensure that hardware manufacturers have the ability to protect the devices and data of consumers.

Art. 6.1(c) currently provides an allowance to maintain restrictions on sideloading to protect "the integrity of the hardware or operating system". That allowance should be expanded to cover measures taken to protect consumer privacy and data security; prevent fraud and distribution of harmful or otherwise illegal material; and comply with intellectual property and other laws. Art. 6.1(f) should include a parallel allowance of measures that restrict access to certain services and technologies for these purposes. And both provisions should make clear that the proportionality test for these measures should take account of the nature and level of risk and the level of protection sought by consumers.

Art. 6.1(f) should focus on fair conditions of competition between first and third party apps. It should not dictate that competition considerations be addressed through particular technical solutions such as direct access and interoperability, which could create significant risks for consumers. Rather, it should leave space for engineers to design competitively equivalent or comparable interfaces that achieve the purpose of the DMA while also protecting the security of consumers' data and the integrity of their devices.

Notes

[1] https://developer.apple.com/documentation/avkit/accessing_the_camera_while_multitasking

[2] Hackers recently used this sort of vulnerability to mass-erase Western Digital hard drives. https://www.forbes.com/sites/leemathews/2021/06/27/a-mysterious-cyberattack-is-completely-erasing-western-digital-mybook-live-drives/

[3] BSI: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Basisschutz-fuer-Computer-Mobilgeraete/Schutz-fuer-Mobilgeraete/Sicherheit-bei-Apps/sicherheit-bei-apps_node.html;

ENISA: https://www.enisa.europa.eu/publications/info-notes/vulnerabilities-separating-reality-from-hype;

DHS: https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf

[4] https://www.dhs.gov/sites/default/files/publications/4681_evaluatingmobileappvettingintegrationwithemm-clean-r4-508c.pdf

[5] Nokia Threat Intelligence Report 2020: https://pages.nokia.com/T005JU-Threat-Intelligence-Report-2020.html?_ga=2.46121956.1346706399.1619200364-2091048293.1619200364

Juan Andrès Guerrero Saade, Principal Threat Researcher at SentinelOne and an Adjunct Professor of Strategic Studies at Johns Hopkins School of Advanced International Studies (SAIS), and Chris Rohlf, Research Fellow at Georgetown's Center for Security and Emerging Technology (CSET): *"SafetyNet and Google Play attempted to tackle the ecosystem integrity problem but largely did not succeed, at least not in terms of widespread malware and exploitation in mobile … At the end of the day, the real issue is that the Android ecosystem is too fractured to address these issues….. Apple has succeeded in blocking a whole swath of attacks — nuisance malware, financial threats, etc. The App Store isn't perfect but credit where credit is due…. As far as iOS goes, we are worried about the top tier of attacks…. But you can't be in a position to only have a top tier problem without first tackling the less sophisticated "here install this APK" style vulnerabilities…. A wider swath of middle-tier actors are doing plenty on Android at a fraction of the investment it would take them to enter the iOS space at all."*

https://twitter.com/juanandres_gs/status/1417178235587211268

[6] Gus Hosein, Privacy International: *"PI's investigations into data brokers and ad tech companies reveal a complex, fast-growing industry that is opaque to the average user. Where there is a lack of transparency, exploitation thrives. Invisible and gratuitous data collection leaves users unable to exercise their rights and protect their privacy. Apple's nutrition labels require industry to be clear and upfront with consumers, and tools like App Tracking Transparency will help people to assert control over the invisible leakage of their data. With these commendable innovations, industry will finally feel pressure to change."*

Jeff Chester, Center for Digital Democracy: *"Apple's new data privacy tools ensure that people have greater control over their personal information. Data brokers and online advertisers will now have to act more responsibly when dealing with consumers who use third party applications on Apple devices."*

https://www.apple.com/newsroom/2021/01/data-privacy-day-at-apple-improving-transparency-and-empowering-users/