Coalition for APP FAIRNESS

SHOULD IOS USERS BE ALLOWED TO DOWNLOAD APPS THROUGH DIRECT DOWNLOADS OR THIRD-PARTY APP STORES?

An analysis of Apple's recent claims

On 13 October 2021, Apple issued a report explaining that allowing users to downloads apps *"through direct downloads and third-party app stores would cripple the privacy and security protections that have made iPhone so secure, and expose users to serious security risks."* Three weeks later, Apple's SVP of software engineering, Craig Federighi, reiterated the same point with force in a keynote speech devoted to security and privacy at Web Summit 2021. Federighi compared regulatory initiatives seeking to open the App Store and iOS to forcing consumers to *"weaken the security of [their] home,"* portraying the process of sideloading apps as *"cybercriminal's best friend."* Apple's position is thus that the only way to protect the safety of iPhone users is to prevent them from downloading apps on their iOS devices through means other than the Apple App Store.

While no one would deny that device security is of paramount importance, **the problem with Apple's position is that it sounds terribly self-serving**. As the only allowed conduit for iOS devices, the App Store is an ever-growing source of revenues for Apple (about $15-20 billion according to various estimates), as Apple charges app developers a 30% commission (in some instances reduced to 15%) on the sale of digital goods and services. By forcing these app developers to use its in-app payment system ("IAP"), Apple is also able to collect valuable information on the app users (name, credit cards details, address, etc.) and confiscate the customer relationship. Apple generates additional App Store revenues by charging developers for search ads which they buy to increase discoverability on the App Store, which some analysts predict will reach $5 billion by the end of this fiscal year. Thus, allowing alternative distribution channels on iOS devices such as direct downloads or third-party app stores could create a dent in Apple's App Store revenues. It would also reduce Apple's ability to gather via IAP commercially sensitive data on apps that sell digital goods and services, including competing apps.

But even assuming that Apple's intentions were entirely pure, Apple's policy would still raise the question of why the security of iPhones can *only* be ensured by having the App Store as the only distribution channel – or to use legal parlance, whether there would be less restrictive alternatives to ensuring security. Most security

features for iOS are built in the operating system and/or the hardware itself, that is they do not depend on the method of app distribution. An example of such a feature is the sandboxing feature that restricts apps from accessing contents of other apps or the system itself. Apple's main argument is that these system-level protections do not suffice to protect against social engineering attacks (e.g., phising), to the effect that there is a need for an additional layer of protection based on human review – the App Store review process. Whether the App Store review process succeeds in that is debatable, since in fact it has not prevented various fraudulent apps from making it to iOS devices. Yet even on the assumption that human review is necessary, the discussion below explains that such review may take place **regardless of the app distribution method**. Apple gives the impression that app review is necessarily linked to the App Store as a distribution channel, but in fact the two can be decoupled.

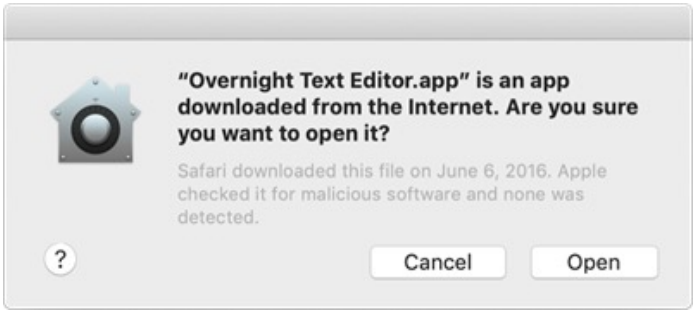
In its above-mentioned report, Apple condemns as unsafe not only direct downloads, but also **downloads from alternative app stores**. This essentially posits that any alternative app stores that Apple would have to allow on iOS devices because it would be obliged to do so by regulation would be incapable of ensuring adequate security. But this position ignores that both the Digital Markets Act and the Open App Markets Act, which in their current version, require Apple to open its devices to third-party app stores, would also allow Apple to take necessary and proportionate measures to ensure the integrity of the device. Specific language can be found to that extent in both Article 6(c) of the DMA (both in the third compromise text of the Slovenian Presidency and the IMCO proposal) and Section 4 of the Open App Markets Act. Thus, nothing would prevent Apple from imposing necessary and proportionate security obligations on third-party app stores to ensure that apps downloaded from their app stores do not undermine the security of the device.

Apple's position seems however to be that third-party app stores are inherently untrustworthy, but that seems hardly credible. There is no reason why third-party app stores would not be able to comply with necessary and proportionate security obligations designed to ensure the safety of the device. After all, while Apple is tightly integrated, it still needs to rely on third-party suppliers to supply a wide range of components or services to build or operate iOS devices. For instance, for a long while Apple relied on third-party chipsets (e.g., produced by Qualcomm) to power its devices. Similarly, Apple relies on third-party payment service providers ("PSP") to process the in-app payments made through IAP. In such cases, we can safely assume that Apple took reasonable steps to ensure its component and service providers comply with requirements designed to ensure the security of the device. Provided that necessary and proportionate measures are in place, there is no reason to believe that Apple has some magic powers that would solely allow it to protect the device security.

As far as **direct downloads are concerned**, Apple's position that they would necessarily create major security risks is also questionable. For one, **Apple allows direct downloads on its Mac computers, while protecting security through a process of notarization**. In a document available on its website, Apple explains to developers how notarizing macOS software *"gives users more confidence that the Developer ID-signed software you distribute has been checked by Apple for malicious components." According to Apple, the notary service "is an automated system that scans [the] software for malicious content, [and] checks for code-signing issues."*

If the scanning of the software reveals there are no issues, the notary service then generates a ticket for the developer to staple to its software, while *"the notary service also publishes that ticket online where Gatekeeper can find it."* [Note: Gatekeeper is an Apple tool that enforces "code signing" and verifies downloaded applications before allowing them to run.] When the user first

installs or runs the software downloaded from the Internet, the presence of a ticket tells Gatekeeper that Apple notarized the software, which *"then places descriptive information in the initial launch dialog to help the user make an informed choice about whether to launch the app."*



On the basis of the information provided in the above box, the user can decide to proceed with the app or cancel. While it is technically possible to download an app that has not been notarized, it is subject to considerable friction as users need to go to their settings and take several steps to make it possible to download the app.

In sum, apps can be downloaded from the Mac App Store in a totally frictionless manner as Apple considers these apps safe. Second, users can download an app from the Internet, in which case two scenarios can arise:

- Either the app has been notarized, in which case the user will be able to download the app with limited friction, in that they will see a box with a warning message and make an informed decision; or
- The app has not been notarized, in which case the user may still download the app but subject to considerable friction.

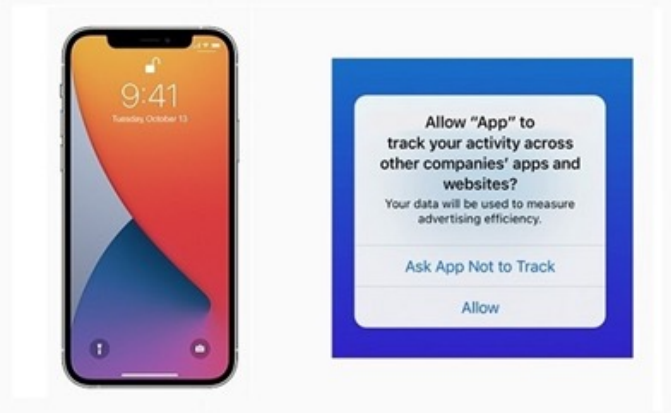
When asked by Judge Yvonne Gonzalez Rogers in the Epic Games v. Apple trial why the iPhone should be treated differently from the Mac, Mr. Federighi replied that "today we have a level of malware on the Mac that we don't find acceptable, and it is much worse than iOS." That is a rather striking statement considering that on its own website Apple says with respect to the Mac that *"Now apps from both the App Store and the internet can be installed worry-free. App Review makes sure each app in the Store is reviewed before it's accepted. And Gatekeeper on your Mac ensures that all apps from the internet have already been checked by Apple for known malicious code — before you run them the first time. If there's ever a problem with an app, Apple can quickly stop new installations and even block the app from launching again."*

There is thus a tension between what Apple says in its marketing materials and Mr. Federighi's statement about the unacceptable level of malware on the Mac. Surely, Apple – who claims to have the most secure ecosystem – would not have allowed Mac users to download apps outside the Mac App Store for so many years if this had endangered the security of their devices. In fact, as pointed out by a commentator, Apple is so keen to keep control of the iPhone that it is willing to throw the Mac under the bus. Unsurprisingly, Judge Gonzales Rogers afforded Mr. Federighi's testimony little weight on this topic, noting that his Mac malware opinions *"appear to have emerged for the first time at trial which suggests he is stretching the truth for the sake of the argument."*

As to the argument that iPhone users store more sensitive and personal information on their iPhone than they would do on their Mac, it is hardly credibly considering that both types of devices can be used to engage in emailing, e-banking, and a wide range of other activities that users expect to perform in secure environments. After all, a user's Mac has access to most sensitive and personal information from the iPhone (e.g., photos, messages) through iCloud syncing.

Similarly, while Apple was willing to trust Apple Mac users to make an informed choice when downloading an app outside the Mac App Store, it now considers in the abovementioned paper that allowing users to decide whether it is safe to download an app outside the App Store would be an onerous burden to put upon iPhone users as they *"would now be responsible for determining*

whether sideloaded apps are safe, a very difficult task even for experts." This proposition should be seen suspiciously for at least two reasons. First, the purpose of notarization is to properly inform users before they take a decision to download an app. If Apple considers that this process is insufficient to ensure device security, it could certainly improve or even take the radical step of banning apps that have not been notarized (in which case steps would have to be taken to ensure that this process takes place in an objective manner, perhaps entrusting it to a neutral third-party). Moreover, Apple's position here contrasts with its strong belief in empowering users to decide over their privacy and the use of their data as recently illustrated by its App Tracking Transparency ("ATT") feature, which prompts users to permit the app developer to "track" them across other companies' apps and websites.



Thus, depending on where its interests lie, Apple seems to have a flexible view on the ability of users to make informed choices over issues affecting the use of their devices.
In any event, even if one assumes that notarization on Mac provides less protection compared to security controls on iPhones, this is only because in its current form, Mac notarization is apparently limited to automated scanning and does not include human review. Y**et there is nothing precluding Apple from adding an element of human review on notarization, to the extent this is necessary.** App distribution can be decoupled from app review, so that the latter may take place regardless of the method of distribution. As Judge Gonzalez Rogers observed in *Epic Games v. Apple*,

"Apple initially considered using app signing for security while allowing developers to distribute freely on iOS. As one document explains, '[app][s] igning does not imply a specific distribution method, ***and it's left as a policy decision as to whether signed applications are posted to the online store, or we allow developers to distribute on their own.'"*** (emphasis added)

Judge Gonzalez Rogers further noted that *"[a]s Mr. Federighi confirmed at trial, once an app has been reviewed, Apple can send it back to the developer to be distributed directly or in another store."* Against this background, it is extremely hard to see how Apple may justify its app distribution restrictions on security considerations. There is no need for centralized app distribution to ensure security. A process of notarization similar to that deployed for Mac – coupled with human review, to the extent strictly necessary – would suffice to ensure security, while allowing for alternative distribution channels such as direct downloads or third-party app stores.

This is not to suggest that notarization is the only way forward to ensure the safe downloading of apps from the Internet or third-party app stores (alternative paths have been suggested; see, e.g., here), but it at least shows that alternative approaches can be explored to protect user security. In fact, the anticipated adoption of the DMA and other legislation seeking to open mobile ecosystems to competition will trigger further research on more competitively-neutral ways to ensure device security.

BY DAMIEN GERADIN

Professor of competition law & economics, Tilburg University ; Partner, Geradin Partners, Brussels ; Outside antitrust counsel to the Coalition for App Fairness (https://appfairness.org/).