Goodbye, walled garden: Apple gets bitten right in the app store

If we are going to bust open the castle walls with the proverbial antitrust dragon, then we will need the right tools and services in order to reduce any possible end-user carnage. 

By Jason Perlow for Tech Broiler | May 13, 2019 - ZDNet

In a landmark decision, the US Supreme Court ruled that a group of iPhone owners can proceed with a lawsuit against Apple on the grounds that the company is engaging in monopolistic practices in its use of a "walled garden." Applications for the iOS platform can only be bought from Apple's app store.

Google's Android platform has historically differed from Apple's iOS in that it has always permitted end-users to "side-load" applications, which include alternative app stores, such as Amazon's.

However, one of the biggest complaints about Android is how easy it is for a third-party, side-loaded application to cause problems on an end user's mobile device. This Android feature includes a risk of creating an overall app

and OS instability -- and potentially allowing malware to install itself.

Apple has allowed side-loading, but only for enterprises using the Developer Enterprise Program. This program enables companies to create and deploy custom applications on iOS, WatchOS, and TVOS devices, as well as code-sign Mac apps, plug-ins, and installers with a Developer ID certificate for distribution to employee Mac computers. As with iOS, Mac also has an app store, but Apple does not require that Mac systems exclusively install applications from it.

While iOS does not currently have this feature, current versions of MacOS use a subsystem called "Gatekeeper," which is a security feature used to enforce code-signing using digital certificates. Gatekeeper verifies the signature of downloaded applications to ensure they are notarized before allowing them to execute, thus reducing the likelihood of inadvertently installing and running malware on the system.

While the Developer Enterprise program has dramatically helped reduce the amount of malicious software installed on iOS systems, it is not infallible. The "Exodus" spyware, which managed to be installed directly from Google Play on Android devices, has been distributed using the Developer Enterprise toolsets on iOS devices.

Although this ruling by the Supreme Court is not a judgment against Apple -- the Court did not classify the company as a monopoly, and it is not moving forward with any antitrust penalty -- the decision does does set a potentially damaging precedent for the company.

By allowing this lawsuit to move forward, it opens up the possibility that there could be, at some point, antitrust proceedings against the company if it continues to maintain a status quo of only allowing Apple-trusted applications from its app store.

EU LOOMS

Additionally, in the past, EU has taken cues from the US whether to move with antitrust proceedings of its own and has also levied severe fines and penalties when it believes its own citizens and corporations are threatened by monopolistic practices of US technology companies.

Case in point: In 2010, EU found that Microsoft had used its market dominance to pre-load its Internet Explorer browser on Windows. In addition to hefty fines, the EU required Microsoft to separate its Internet Explorer browser from the operating system and allowed the consumer to choose which web browser could be installed on the OS during the initial set-up process. Microsoft maintained a website called BrowserChoice.eu for this purpose, which was hosted until early 2015.

Another example: In July 2018, the EU levied a $5 billion fine against Google for anti-competitive behavior on its Android OS. As part of the EU ruling, Google must stop forcing Chrome and Google search on Android OEMs, and prevent any efforts to block forked versions of Android.

If you think $5 billion of fines against Google sounds bad for default search engine choices, wait until you see what it decides to do to Apple for alleged monopolistic practices with its app store.

I believe that Apple's best strategy, going forward, is to port the Gatekeeper process/subsystem to iOS, WatchOS, and TVOS, and to create a digital signing infrastructure for third-party applications, which would include third-party app stores and installable application packages.

I also think some cloud-based application package management system -- similar to what enterprises use for their developer accounts to install third-party apps -- should be made available to consumers that can be purchased as a value-added service. Additionally, Apple should not be obligated to provide cloud-sync or data backup infrastructure to side-loaded apps or app stores.

Cyber attacks and malware are one of the biggest threats on the internet. Learn about the different types of malware - and how to avoid falling victim to attacks.

Part of allowing side-loaded apps onto iOS is also going to be allowing these apps to have the same privileged status to access native APIs and other services on the OS. To me, that is troubling, because it opens up the potential for a lot of platform abuse.

A lot of the value proposition of iOS is that it is a relatively safe platform, and that has been mostly resistant to malware attacks, although some malicious app store apps have been found, notably ones that communicate with Command and Control (C2) infrastructure of threat actors.

Any allowing of side-loading on the iOS platform has to come with a big warning and waiver of responsibility to the end user, just as it is issued on Android. Maybe even two levels of "Are you sure?", with password/ID verification. While allowing side-loaded apps and app stores onto the iOS platform could be fraught with problems, and introduce many undesirable variables into the overall user experience, I do think it has some potential benefits.

Third-party app stores have not been an enormous boon for Android, in terms of revenue generated in commercial software development, but it has allowed for increased choice for the end-user, particularly as it relates to adult content and other things that Google itself deems inappropriate or goes against its self-interests.
There are many kinds of applications that could benefit from side-loading on iOS. One such example could be

payment systems that might compete with Apple Pay, such as Google Pay, which exists on the iOS platform but doesn't currently have NFC capabilities, likely due to concerns of being delisted in the app store, if that functionality was enabled.

Samsung chose not to launch its Samsung Pay app and service on iOS, likely due to the difficulty of being listed on the app store. If side-loading were permitted, not only could Samsung launch its payment service on iOS, but potentially its app store, as well.

Another third-party app store that may be of interest to broader use is Cydia, which is currently used by users of "jailbroken" iOS systems. But these are more along the lines of tweaks and hacks to extend iOS, for those who want to customize their user experience. Third-party side-loading would not be akin to jailbreaking (sometimes referred to as "rooting"), in which low-level OS services and settings could be changed that are generally not accessible to an end-user.

I believe it is inevitable that iOS' walled garden will be demolished. But if we are going to bust open the castle walls with the proverbial antitrust dragon, then Apple should provide the needed tools and services in order to reduce any possible carnage -- as well as issue appropriate advisories to its end-user population (that

perhaps opening those application gates for most people might not be such a great idea).

original article: https://www.zdnet.com/article/goodbye-walled-garden-apple-gets-bitten-right-in-the-app-store/?ftag=TREc64629f&bhid=23405847687286447375579737817622