The Curation Chokepoint

James Larus

Abstract A key rationale for Apple and Google’s app stores was that they curate apps to ensure that they do not contain malware. Curation has gone beyond this goal and now unduly constrains the apps that you can use on your smartphone. It needs to stop. App quality should be ensured with other techniques and by a wider range of organizations than just Apple and Google.

Imagine if you can a dystopia in which your landlord decides the food you can bring home to your apartment, either to cook or eat. Or that a manufacturer decides if a movie will play on your TV. Further imagine that your landlord and TV manufacturer demanded 30% of your grocery budget and Netflix subscription price for this “service.”

This scenario seems absurd. However, it is the current situation on your smartphone. Apple and Google are a duopoly that wrote the low-level software (the operating systems iOS and Android) that control virtually all smartphones throughout the world. Apple and Google decide which apps can be installed on your smartphone, and they charge for this service.

Both companies operate an online “app store” that is the chokepoint in the distribution of apps. Apple iPhones can *only* install apps distributed by Apple’s App Store.¹ Google permits alternative app stores but heavily promotes and favors its Play Store (e.g., it is pre-installed and using another app store may require changing a setting). Both companies’ app stores heavily curate the apps they accept, and both charge a 30% commission on purchase of apps and on subsequent purchases performed within the apps themselves.

Neither company’s app store makes any pretense of being a neutral marketplace. Listing an app in either store requires agreeing to a contract with precise terms

¹ Apple makes an exception to allow companies to write and distribute software on smartphones that they own.

J. Larus (✉)
EPFL, Lausanne, Switzerland
e-mail: James.larus@epfl.ch

specifying the allowed types of apps, permissible software development techniques, and details of how an app operates. Companies developing apps have long chafed at the heavy-handed and anti-competitive operation of these stores, but they have done so quietly for fear of retaliation. This concern is real and based on both companies' heavy-handed ways of resolving disputes, which start by using the vast disparity in negotiating strength to remove a contested app from the app store, thereby cutting off a developer's revenue. Recently, emboldened by governmental investigations in the USA and Europe, some companies have gone public with their disputes and complaints:

- Spotify, the Swedish online music streaming service, filed an anti-trust complaint with the EU, accusing Apple of unfair competition because it charges Spotify 30% of its subscription revenues. Apple distributes its competing Apple Music app pre-installed on iPhones without a fee (Satariano and Nicas 2019).
- The Swiss privacy software firm ProtonMail complained about the 30% fee and also that Apple insisted it remove the statement that its VPN app “unblock [s] censored websites” (Yen 2020). They further complained that Apple threatened to remove their email client app from the App Store unless they added an in-app purchase of email accounts, so that Apple could charge a commission. After agreeing to Apple's demand, ProtonMail raised the price of their email by 30%.
- Apple rejected an app that monitored Tesla cars' information because it used an unofficial library to extract data from a car. Apple claimed that the app developer needed approval from Tesla to use this library in its app (Espósito 2020).
- The developer of the popular Fortnite game, Epic Games, filed a lawsuit against Apple for anti-trust violations for requiring the use of Apple's payment system for in-game purchases, with its 30% commission (Nicas 2021). After the suit, Apple removed Fortnite from its App Store. A similar complaint against Google led to Fortnite's removal from Google's Play Store and a similar lawsuit.
- Facebook added a COVID-related service that allowed Facebook users to purchase online classes, with all revenue going to the business. Google allowed this, but Apple charged a 30% commission and prohibited the app when Facebook added a note informing the consumer that “Apple takes 30% of this purchase” (Lee 2020).
- Apple rejected gaming apps from Facebook and Microsoft because they were arcades that allowed subscribers to download and play games not installed through the App Store.

While considerable public attention has focused on the 30% commission and anti-competitive practices of the app stores, this chapter focuses on a different, fundamentally harmful consequence of Apple and Google's app stores. A key rationale for these stores is that both companies curate apps to ensure that they do not contain malware (software that subverts a computer or steals information). This vetting

process is valuable and practical, as malware is far rarer on smartphones than on computers.²

Detecting malware is technically challenging. The fields of computer security and program analysis have developed numerous techniques for identifying malevolent programs, but the most active and creative malicious adversaries are typically one step ahead. Apple's rules for submitting apps to the App Store have a clear intent of facilitating code inspection, for example, by limiting apps to using published APIs and libraries, not downloading libraries or code, and not using interpreted code. The inspection process details are confidential, but Apple's documentation suggests it consists of automatic inspection of an app's code and manual execution to explore and approve its behavior.

While Apple's efforts may have raised most apps' quality level, it has not deterred sophisticated hacking groups such as NSO, whose spyware has been used by governments to track activists (Kirchgaessner and Safi 2020; Wolff 2019). NSO's Pegasus spyware used flaws in Apple's iMessage app (pre-installed) and Facebook's WhatsApp (App Store) to install spyware used by Middle Eastern countries to track political opponents and reporters. It is not surprising that curation is imperfect; one of the first and most profound theoretical results in computer science, Turing's Halting Problem, established that it is impossible to prove most non-trivial properties of computer programs. Program defect detection and security analysis rely on approximate analysis, which inherently suffers from false positives and missed errors.

The legal discovery process in Epic's lawsuit against Apple documented that the review process was cursory. In 2016, reviewers spent 13 min per new app (6 min per updated app) and were expected to review 50–100 apps per day (Epic Games 2021). The *Financial Times* quoted Eric Friedman, head of [Apple's] Fraud Engineering Algorithms and Risk (Fear) unit, that the process was "more like the pretty lady who greets you . . . at the Hawaiian airport than the drug-sniffing dog" and assessed the App Store's defenses against malware as "bringing a plastic butter knife to a gunfight" (Chung 2021).

It turns out that, once malware is installed on an iPhone, Apple's strong isolation and restrictive rules shield it by, paradoxically, preventing the creation and distribution of effective anti-virus protection apps for iOS (O'Neill 2021).

Moreover, malicious adversaries can take advantage of Apple's ahead-of-time approval process, which examines an app before distribution and does not monitor its subsequent behavior on smartphones, to exhibit one face to Apple and another, less benign one to users (a violation of Apple's license agreement, but a malware vendor need not abide a license).

²Apple, in its Proposed Findings of Fact and Conclusions of Law, in Epic's lawsuit asserts: "the iPhone platform accounted for just 0.85% of malware infections. DX-3141 at 15. By contrast, Android accounted for 47.15% and Windows/PC accounted for 35.82%" (Apple 2021).

Apple's approach of claiming exclusive control over security and depending on App Store curation and isolation mechanisms on iPhones runs against the grain of centuries of security experience demonstrating the need for defense-in-depth.

More importantly, why should Apple determine which software is innocuous for all consumers who purchase an iPhone? Perhaps my risk tolerance is higher than average, and I want to try apps from developers who push the boundaries of what is possible on a phone and need to use libraries and techniques that Apple cannot inspect and so prohibit. Or perhaps my aesthetic sensibilities differ from the premise of the App Store, "The guiding principle of the App Store is simple—we want to provide a safe experience for users to get apps . . . We have lots of kids downloading lots of apps. . . ." Or perhaps I am a developer who runs afoul of Apple's self-admittedly vague and arbitrary standards:

We strongly support all points of view being represented on the App Store, as long as the apps are respectful to users with differing opinions and the quality of the app experience is great. We will reject apps for any content or behavior that we believe is over the line. What line, you ask? Well, as a Supreme Court Justice once said, "I'll know it when I see it." And we think that you will also know it when you cross it. (Developer [n.d.](#))

In the end, the fundamental question is whether the manufacturer of *my* phone should have the right to deny *me* the ability to install an app on *my* phone, and, conversely, the right of a software developer to produce and distribute an app, even if Apple finds the app inappropriate or offensive. I think that most reasonable people would say no.

Apple provides a valuable service by offering a curated collection of apps, much as Disney provides a service by providing entertainment appropriate for an entire family. However, no one, including Disney Corporation, would contend that their products encompass the full spectrum of entertainment or satisfy all tastes. Nor does it need to, as there are many other ways in which movies and television are produced and distributed.

The valuable aspect that Apple offers (malware protection) is achievable in other ways. Google's Android operating system allows alternative app stores. It is easy to envision an ecosystem of app stores, which offer software along with guarantees of its provenance (e.g., it is produced by a small firm that we know), application of an App Store-like inspection process, or even stronger techniques of program analysis (e.g., we inspected the source code of the application and built it ourselves). In many other domains, quasi-public organizations (e.g., UL in the USA or CE certification in Europe³) attest that a product meets publicly approved standards.

Moreover, Apple should not rely on a single mechanism (ahead-of-time App Store inspection) to provide security, as demonstrated by NSO malware. The "sandbox" mechanism on the iPhone, which isolates an app and controls the smartphone features it can access, needs further strengthening and restructuring to

³Underwriters Labs (UL) is a company that provides safety testing and certification of products, particularly for the USA. CE certification indicates that a product sold in the European Union conforms to EU health, safety, and environmental protection standards.

allow a phone's user to control over its operation. A sandbox can prevent an app from accessing the user's private information, such as their address book, using privacy-revealing mechanisms such as GPS, or communicating outside of the phone with a radio or WiFi. It is a powerful mechanism for controlling what runs on smartphones, too powerful to be left entirely in Apple and Google's hands.

A phone's owner should use these mechanisms to impose restrictions that conform to their desired risk level and expected behavior. A 15-year-old teenager may want to try edgy new apps and not be particularly concerned about personal privacy. A 45-year-old CEO is likely to be genuinely concerned about their work phone's security but more relaxed about their personal phone. One size does not fit all.

Apple and Google provide a valuable service by offering carefully inspected apps. This initial motivation made the app stores and smartphones successful and provided both companies with powerful commercial leverage to control and financially exploit the companies that write software for their phones. As governments increasingly examine these practices, it is essential not to lose sight of these app stores' stated motivation. Curation to exclude malware can be done in many ways and by many parties, and curation by content is only justified if alternative distribution mechanisms exist and are equally accessible.

References

- Apple. 2021. "Apple Inc.'s Proposed Findings of Fact and Conclusions of Law." Case 4:20-cv-05640-YGR. https://www.scribd.com/document/502037049/21-04-07-Apple-Proposed-Findings-of-Fact-and-Conclusions-of-Law#from_embed.
- Chung, Jean. 2021. "Apple Engineer Likened App Store Security to 'Butter Knife in Gunfight.'" *Financial Times*, April 9, 2021.
- Developer, Apple. n.d. "App Store Review Guidelines." Accessed February 19, 2021. <https://developer.apple.com/app-store/review/guidelines/>.
- Epic Games. 2021. "Findings of Fact and Conclusions of Law Proposed by Epic Games, Inc." https://www.scribd.com/document/502036985/21-04-08-Epic-Games-Proposed-Findings-of-Fact-and-Conclusions-of-Law#from_embed.
- Espósito, Filipe. 2020. "Apple Rejects 3rd-Party Tesla App Update as It Strictly Enforces Written Consent for Third-Party API Use." *9To5Mac*. August 27, 2020. <https://9to5mac.com/2020/08/27/apple-rejects-watch-for-tesla-app-as-it-starts-requiring-written-consent-for-third-party-api-use/>.
- Kirchgaessner, Stephanie, and Michael Safi. 2020. "Dozens of Al Jazeera Journalists Allegedly Hacked Using Israeli Firm's Spyware." *The Guardian*, December 20, 2020, sec. Media. <http://www.theguardian.com/media/2020/dec/20/citizen-lab-nso-dozens-of-aljazeera-journalists-allegedly-hacked-using-israeli-firm-spyware>.
- Lee, T. B. (2020). Apple backs down on taking 30% cut of paid online events on Facebook. <https://arstechnica.com/gadgets/2020/09/apple-backs-down-on-taking-30-cut-of-paid-online-events-on-facebook/>
- Nicas, J. (2021). Apple Fortnite Trial Ends with Pointed Questions and a Toast to Popeyes, <https://thecollegesave.com/2021/05/25/apples-fortnite-antitrust-trial-ends-with-pointed-questions-2/>.

- O'Neill, Patrick Howell. 2021. "How Apple's Locked down Security Gives Extra Protection to the Best Hackers." *MIT Technology Review*, March 31, 2021. <https://www.technologyreview.com/2021/03/01/1020089/apple-walled-garden-hackers-protected/>.
- Satariano, A and Nicas, J. (2019). Spotify Accuses Apple of Anticompetitive Practice in Europe, *The New York Times*.
- Wolff, Josephine. 2019. "Whatever You Think of Facebook, the NSO Group Is Worse." *The New York Times*, November 6, 2019. <https://www.nytimes.com/2019/11/06/opinion/whatsapp-nso-group-spy.html>.
- Yen, Andy. 2020. "The App Store Is a Monopoly: Here's Why the EU Is Correct to Investigate Apple." *ProtonMail Blog* (blog). June 22, 2020. <https://protonmail.com/blog/apple-app-store-antitrust/>.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.