Judge says Apple may be ‘stretching the truth’ on Mac malware concerns

During the *Apple v. Epic* trial, Apple software leader Craig Federighi argued that tight control over the App Store was necessary for securing the iPhone. But Judge Yvonne Gonzalez Rogers didn’t buy it, writing in her ruling Friday that he may have been “stretching the truth for the sake of the argument.”

Federighi cast heavy doubts about whether Apple would be able to secure iPhones without its App Review system acting as a gateway, by saying that the macOS security was basically in a bad place. Judge Rodgers doesn’t think Federighi has the proof to back it up (you can read her quotes below in context on page 114):

> *While Mr. Federighi’s Mac malware opinions may appear plausible, they appear to have emerged for the first time at trial which suggests he is stretching the truth for the sake of the argument. During deposition, he testified that he did not have any data on the relative rates of malware on notarized Mac apps compared to iOS apps. At trial, he acknowledged that Apple only has malware data collection tools for Mac, not for iOS, which raises the question of how he knows the relative rates. Prior to this lawsuit, Apple has consistently represented Mac as secure and safe from malware. Thus, the Court affords Mr. Federighi’s testimony on this topic little weight.*

Woof. Basically, Judge Rodgers says that Federighi was trying to make the Mac look bad so iOS could shine, without much

evidence. After discussing notarization and App Review a bit more, she concludes that Apple could implement a system similar to the Mac's without giving up much of the security iOS already enjoys:

> *Ultimately, the Court finds persuasive that app review can be relatively independent of app distribution. As 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. Thus, even though unrestricted app distribution likely decreases security, alternative models are readily achievable to attain the same ends even if not currently employed.*

It's worth keeping in mind that Judge Rogers didn't end up forcing Apple to allow alternative app stores or side-loading, and that this opinion is only contending one of Apple's points. But it's sharp criticism of Apple's more prominent defenses of its locked-down approach to iOS.

Epic argued at trial that Apple could achieve security and privacy on iOS without controlling the exclusive way to distribute apps. It suggested that Apple could use a system similar to the Mac – by scanning apps before they run, and checking to see if it's the same code that Apple has notarized. While the Mac notarization process doesn't currently include all of the checks that happen in App Review, in theory it could if Apple wanted it to.

Federighi strongly disagreed that this would be sufficient. He argued that iPhones have more sensitive data than Macs do, that the iPhone's popularity makes it a bigger target than Macs, and that Mac users have basically just learned to be more careful when installing apps. He also argued separately that Apple isn't happy with where security is on macOS, and said that adopting the same security model would be a "very bad situation for [Apple's] customers."

Judge Rodgers argues against Apple’s stance that third-party app installations or app stores would seriously harm iOS’s security. The Mac’s Notarization system currently doesn’t keep away the kinds of problems that App Review does (or, at least, is supposed to), but there’s no reason why it couldn’t. Even if Apple doesn’t want to implement it onto iOS, perhaps it could consider taking her suggestions to heart if its unhappy with the state of macOS security.

https://www.theverge.com/2021/9/10/22667256/apple-vs-epic-trail-judge-craig-federighi-macos-security-arguments-iphone-ios-response