Google’s Response to Working Paper #2: The Requirement for Browsers Operating on iOS Devices to Use Apple’s WebKit Browser Engine

31 July 2024

Introduction

1. Google welcomes the opportunity to respond to the CMA’s Working Paper on the requirement for browsers operating on iOS[1] devices to use Apple’s WebKit browser engine (**WP2**).

2. Browser developers rely on browser engines to turn a website’s code into visual elements on the page. They are largely responsible for the security, performance and privacy (**SPP**) features of browsers they are incorporated into.

3. Under section 2.5.6 of Apple’s App Store Review Guidelines, “*Apps that browse the web must use the appropriate WebKit framework and WebKit Javascript*.”[2] This requires all browser apps on iPhones and iPads to use Apple’s WebKit browser engine, and prevents them from making modifications to it. WP2 states that Apple “*excludes all competition between browser engines on iOS*.”[3]

4. This response explains, from our perspective, how browser engine choice on a mobile platform:

   - Can facilitate greater competition on SPP (**Section I**).

   - Can advance the web ecosystem by reducing incompatibilities between browsers on different platforms (**Section II**).

   - Does not necessarily compromise security (**Section III**).

I. Browser Engine Choice Facilitates Browser Competition Based on SPP

5. On Android, browser developers can use any browser engine they want. They can use Google’s Blink browser engine or an alternative like Gecko or Apple’s WebKit. They can even use a mixture of browser engines: Lunascape, for example, is based on WebKit, Gecko, and Trident. This flexibility enables browser developers on

[1] In this response, “iOS” also refers to “iPadOS.”

[2] *See* Apple’s App Store Review Guidelines.

[3] WP2, ¶1.5.

Android to differentiate themselves based on SPP and introduce new innovations to their browsers. In particular:

- **Browser engine choice allows security innovations**. We constantly update Chromium to implement innovative security features and fixes. For example, we have recently launched Trusted Types[4] and TLS Encrypted Client Hello.[5] Site Isolation, one of the major security innovations in browsers in recent years, is not available on Chrome for iOS because it is a browser engine-level feature, and WebKit does not support any equivalent. And we are continuously working on the development of new features to ensure that Chromium and Chrome remain as secure as possible: examples of our pipeline security work include Device Bound Session Credentials[6] and a Digital Credential API, which would enable high-security digital IDs.[7] Much like the other browser vendors that WP2 cites, we are not always able to bring our security innovations to users of iOS.

- **Browser engine choice allows different approaches to privacy**. Privacy is an active area of innovation and differentiation in browsers, with trade-offs and no single best design that should be imposed on all platforms by a platform owner. Browsers like Opera, DuckDuckGo, and Brave, for example, market themselves with a specific focus on user privacy. They are able to make good on that promise on Android where they are able to modify their browser engine code and introduce new or different privacy functionality.

  Similarly, Google has launched enhanced privacy features for Chrome on Android, which we are not currently able to bring to iOS. For example, since September 2023 Chromium has supported TLS Encrypted Client Hello allowing websites to opt-in to avoid leaking sensitive fields, like the server name, to the network.

- **Browser engine choice leads to better performance**. On Android, where browser engine choice is possible, third parties are also entirely free to modify or even 'fork' their Blink-based browser, introduce new features for developers, and innovate above a performance 'baseline'. Our efforts to constantly improve Chrome's performance are reflected on other platforms, where browser engine choice is possible. In 2023, for example, we made improvements to Chromium's speed and efficiency that resulted in a "*10%*

[4] Trusted Types has enabled major websites to virtually eliminate one of the most common types of website security issues - cross-site scripting (XSS) vulnerabilities.

[5] TLS Encrypted Client Hello allows websites to opt-in to avoid leaking sensitive fields, like the server name, to the network.

[6] Device Bound Session Credentials is a feature we are currently experimenting with to detect and mitigate a common attack called "cookie theft"; *see* GitHub, Device Bound Session Credentials explainer.

[7] *See* GitHub, Digital Credentials.

increase in Apple's Speedometer 2.1 browser benchmark over the course of three months."[8] In 2022, Chrome for MacOS achieved the highest scoring results to date on web responsiveness benchmarks.[9] Chrome's users on iOS do not benefit from these improvements unless Apple also chooses to implement them in WebKit.

II. Google Promotes Compatibility Across the Web Ecosystem

6. In Google's response to WP1, we explain our commitment to promoting compatibility across the web ecosystem. As a result of these efforts, Blink consistently outperforms other browser engines on compatibility. It has by far the fewest number of engine-specific web platform test failures. WebKit on iOS is the major outlier to compatibility in the mobile web ecosystem. As WP2 finds, "*WebKit has performed worse in terms of compatibility with [the Web Platforms Tests Project's] tests than Blink and Gecko*."[10] WP2 cites web developers' concerns that they "*face costs from ensuring their websites are compatible with WebKit given its limitations with respect to functionality.*"[11]

7. If browsers could choose a different browser engine on iOS, or could modify WebKit, they could introduce features and reduce incompatibility across the ecosystem. They would not be reliant on Apple to do so. Apple, in turn, would face more pressure to improve WebKit's compatibility on iOS. On macOS, where Apple feels competitive pressure with respect to WebKit, it supports more features. This would benefit browser competition, web developers, and users.

III. Browser Engine Choice Does Not Compromise Security

8. WP2 says the CMA has "*not yet seen clear evidence that the WebKit restriction confers a significant improvement in security compared to a situation where other browser engines would be allowed on iOS*."[12] Having multiple browser engines does not give rise to unmanageable security risks. If all browsers use the same engine—and in particular the same codebase—every device is vulnerable once an attacker has found and developed an exploit. Having browsers based on different codebases, by contrast, may mean that a bug only targets certain browsers and not others. Allowing a variety of browser engines can therefore improve a platform's overall operational resilience.

[8] *See* Chromium Blog, More ways we're making Chrome faster (13 April 2023).

[9] Chromium Blog, A new speed milestone for Chrome.

[10] WP2, Appendix, ¶1.8.

[11] WP2, ¶4.23.

[12] WP2, ¶5.16.

9. Any risk from poorly maintained browsers can be managed while allowing browsers to choose the browser engine they use. In particular:

- **Frequent and flexible security updates**. Chrome on Android pushes a new update to users (often containing security fixes) almost every week, and does so more frequently if there is a specific security need.

- **Policies and standards**. Google supports and actively contributes to policy initiatives and standards on building security into the design of software. Google has implemented various security principles and follows practices to ensure Android is designed to defend users from things like malicious servers and phishing attacks.

- **Targets and monitoring**. Google Play requires new apps and app updates to meet specified targets within one year of the latest major Android OS version release. This ensures users realise the full benefits of the privacy, security, and user experience improvements that each Android OS update brings.

- **Systemic security enhancements**. We use our App Security Improvement Program to improve the security of all apps distributed via Google Play.[13] The program provides tips and recommendations for building more secure apps and identifies potential security enhancements when apps are uploaded to Google Play. To date, the program has facilitated developers to fix over 1,000,000 apps on Google Play.

- **Open systems**. Android's open system means that it can benefit from contributions from the wider developer community. This reduces the chances of a bug or issue not being discovered, and helps identified bugs being fixed quickly.

- **Competition on security parameters**. Having multiple browser engines can foster innovation related to security, performance, stability, and more. In fact, innovation in security (and more) was made possible when Chrome forked WebKit to invest in Blink/Chromium in the first place. User privacy and security are basic parameters on which browsers and browser engines can and do compete.

Conclusion

10. The CMA has already found that there is a "*strong case*" for allowing other browser engines on iOS, something which is currently prohibited by Apple.[14] WP2 states that the WebKit restriction could lead to "*worse levels of security, privacy, performance,*

[13] Developers, App security improvement program.

[14] *See* the CMA's Mobile Ecosystems Final Report, ¶8.126.

and feature support for browsers on iOS."[15] This contrasts with the position on Android where browser engine choice is possible. The CMA's concerns about Apple's WebKit restriction therefore do not apply to Android.

*   *   *

[15] WP2, ¶3.32.