AMENDED Exhibit 1018

PLAINTIFFS' OMNIBUS OPPOSITION TO DEFENDANTS' MOTIONS FOR SUMMARY JUDGMENT

ATTORNEY-CLIENT WORK PRODUCT | NEED TO KNOW

Chrome (Android and ChromeOS) requirements for supervised accounts

Authors: [redacted]
Updated: Jun 2020

Summary

As part of an on-going privacy incident investigation ([redacted]), we have put together this document to summarize the requirements and CUJs involving supervised user experiences in Chrome, as well as our understanding of the features that were built in Chrome to support supervised child accounts on Android and ChromeOS devices. We propose that the Requirements & CUJs should serve as the rubric by which we assess how well the current implementation in Chrome supports the key legal, privacy, and product requirements. Per alignment with the impacted teams, the ownership structure of these CUJs are captured [HYPERLINK "https://docs.google.com[redacted] \h].

Commented [1]: [redacted] Can I get access to this please?
_Assigned to [redacted]

Commented [2]: I don't have access either. Ask [redacted] from incident management team?
Reassigned to [redacted]

Table of Contents

[TOC \h \u \z \n \t "Heading 1,1,Heading 2,2,Heading 3,3,Heading 4,4,Heading 5,5,Heading 6,6,"]

Terminology

Family Link - Google product to enable parents to manage their children's supervised accounts.

Unicorn accounts ("Unicorns") - kid accounts under the age of 13 (or age of consent)

Supervised account - [redacted] [HYPERLINK [redacted] " \h]. [redacted] [HYPERLINK [redacted] \h].

HIGHLY CONFIDENTIAL (COMPETITOR) - EXPORT CONTROL PROTECTED MATERIAL GOOG-3047MDL-05630293.ECM

Supervised devices - Android and ChromeOS devices which enforce identity management to ensure that only the supervised account[1] can be used with a given user profile on the device. As part of this enforcement, signed-out/incognito states in Chrome are disabled. We make no representation for Chrome experiences on non-superviseable devices, as the child can circumvent policy restrictions and parental controls via signed-out states.

Supervised user - user logged into a Google service with a supervised account

Introduction and context

Supervised accounts[2] are Google's response to market demand and regulation (such as COPPA and GDPR) for additional protections over under age-of-consent users around the world. Supervised accounts are active on 22.3M Android and Chromebook devices[3], as well as a large number of non-supervised devices[4]. Android and CrOS operating systems have the means to recognize supervised accounts and enforce operating system-level restrictions on them. Some restrictions are enforced by legal or policy requirements (e.g. no interest-based advertising for children), while others are features offered to parents to manage their children's use of digital devices (e.g. setting up screen time limits and blocking specific apps).

In addition to restrictions that can be applied at the operating system level, some additional restrictions need to also be applied in individual Google products. Chrome is one such product in which special treatment needs to be given to supervised accounts. Before the Unicorn team existed, a team internally known as Playpen in Chrome developed a feature called [HYPERLINK "https://docs.google.com[redacted] \h]. This allowed users to create secondary local Chrome profiles, tied to their own ChromeSync storage, to create a limited environment for children to browse with. This was supported in desktop and ChromeOS versions of Chrome.

As the Unicorn team approached Chrome to support COPPA-compliant accounts, that team pivoted to supporting these use-cases on Android, and for an account added at the operating system level as the single identity on the device[5]. Over the years the need for a

---

[1] With the exception of EDU accounts

[2] There are different [HYPERLINK [redacted] \h] of supervised accounts, but the policy restrictions apply only to Unicorn accounts as those users are under the age of consent.

[3] [HYPERLINK "[redacted]" \h]; the ratio of Android to Chromebook devices is ~99:1

[4] Including iOS, Mac OS, Windows

[5] More precisely in Android platform terms, the single account in a [HYPERLINK "https://support.google.com/nexus/answer/2865483?hl=en" \h] space

- (Geller only) When a previously unsupervised account becomes supervised (a process called *gellerization*), Chrome needs to start enforcing ChromeSync and other rules below

Content safety

By policy, Unicorn accounts cannot access certain Google 1P web services and applications. Notably, Unicorn accounts are blocked from accessing YouTube main. In addition to that, many Google services have special treatment for Unicorn (either blocks or other feature changes).

For services that are blocked, server-side protections such as [HYPERLINK [redacted]" \h] make sure that these services don't work for signed-in Unicorn accounts, and on supervised platforms it should not be trivial to get access to signed-out experiences by tampering with the browser.

This block is enabled in slightly varying methods by each Google domain, [redacted] If the service has not been whitelisted for Unicorn accounts, [redacted]

These server-side protections only work if we can consistently identify the user. So we need Chrome to enforce that the active identity matches the one signed into the supervised platform, for all Google services and not just for *.google.com.

Children should not be able to easily bypass such modified behavior by switching accounts on Chrome, and currently Chrome tries to do this with the following technical and product changes:

- Identity consistency is enforced
- Incognito mode is disabled
- Multilogin on the content area is disabled
- Developer tools are disabled
- Blocking cookies is disabled by default (behavior can be changed by the parent in Family Link)

Browsing restrictions

Web browsing is limited to websites allowed by parents and policy, as detailed in the "Requirements & CUJs" section above.

Parent-managed restrictions

There are three "browsing modes" parents can select from in Family Link:

- 1P services will show ads according to the policy of the account signed into the tab or app
- Chrome browsing data, bookmarks and passwords will be synced to the primary logged in Unicorn Account instead of the EDU account. All other data for tabs where a user is logged into GSFE will be logged to the relevant GSFE core or additional service in accordance with the GSFE privacy notice.

More details are captured in the [HYPERLINK "https://docs.google.com/[redacted] \h] and [HYPERLINK "https://docs.google.com[redacted] \h].

Secondary account sign in with EDU accounts is not yet supported in Chrome on Android.

Other features

- Website permissions such as camera and location are blocked by default (behavior can be changed by the parent in Family Link)
- The parent can remotely clear a child's browsing history (but not see it) in Family Link
- (ChromeOS only) Chrome Web Store and extensions are disabled up until M83
- (ChromeOS only) Parents can set a daily web time limit. Chrome and PWAs will be blocked after the limit is reached (with the exception to allow-listed items)..

Commented [redacted] that is relevant for Chrome browser.

Known issues

1. Supervised users can use tools in Chrome UI to remove cookies and get around restrictions (e.g., [HYPERLINK "h[redacted]" \h], [HYPERLINK [redacted]" \h])
2. Website blacklisting/whitelisting is flaky (e.g., [HYPERLINK [redacted]" \h], [HYPERLINK [redacted] \h], [HYPERLINK [redacted] \h])
3. Parents have poor comprehension of how to define a domain vs. url sufficiently to achieve the desired behavior in website black/whitelisting (e.g., [HYPERLINK [redacted]" \h]
4. Supervised accounts remain signed-in to Chrome after being removed from the device ([HYPERLINK [redacted]" \h])
5. Website restrictions don't work on webviews (e.g. [HYPERLINK "[redacted]" \h])