

AMENDED Exhibit 884

PLAINTIFFS' OMNIBUS OPPOSITION TO DEFENDANTS' MOTIONS FOR SUMMARY JUDGMENT

Case No.: 4:22-md-03047-YGR

MDL No. 3047

In Re: Social Media Adolescent Addiction/Personal Injury Products Liability Litigation

DOCUMENT SLIPSHEET

P-SNAP-0602

Bates Number: SNAP3664412-SNAP3664415

Custodian: OSBORNE_ALEX

Author:

Filename: AGE ASSURANCE DOC NOTES _ OLD STUFF.DOCX

Create Date: 11/17/2023 12:00 AM

Last Modified Date: 11/17/2023 12:00 AM

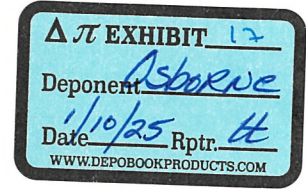
TNAG BEGBATES:

TNAG ENDBATES:

MAAG BEGBATES:

MAAG ENDBATES:

File Path: /AGE ASSURANCE DOC NOTES _ OLD STUFF.DOCX



Age Assurance doc notes / old stuff

Everything below will be deleted

Meeting Notes

Things to follow up on still

- Create four options
- Figure out right way to sequence this and make sure we present our case in the best way possible
- Follow up on BIPA consent
- Add new ideas we discussed on Nov 9
- Add in latest EC/EU stuff

Nov 16

- Remove the parental consent thing
- Figure out better cons

Nov 9

- Other things we could add to our menu
 - Should we consider adding a dedicated reporting reason for "This looks like a child" (double check what the other platforms are doing)
 - FB and IG have ways to do this via their webform, so do we. We could incorporate this into the app
 - Ad reporting << when people report "I'm underage why am I seeing this?" << we could add age verification here? (or any case where someone indicates this is inappropriate)
 - Punishing for helping us out
 - Parental consent/age verification via Family Center << include this is a menu
 - Public Profiles << age verify if you want one as U18 (parental consent?)
 - My AI << add age verification? "I'm 12, keep using, verify your age"
- Key Point: as we make Snapchat increasingly cross platform, but especially with the introduction of a fully featured desktop web version of Snapchat, we weaken the argument for the operating system (e.g., iOS) being responsible for age assurance. Therefore, we should really do something ourselves.
- Growth impact of implementing some sort of block on retrying registration << maybe we just figure out how to re-run this test
- Support site reports << any place where we have comments << this would be part of U13 delete appeal
- T&S reports << "I'm 12 I shouldn't see this" << this would be part of the U13 delete appeal

Do this >> Let's present the concept of doing 13-15 PP and doing it via FC << maybe getting this with some "parental consent". Then let's basically say

Nov 2 Meeting Notes

- Key questions to discuss/answer
 - Where else do we need to dig in on the mixed-audience experience?
 - What options do we want to present in this doc?
- **Need a way to explain what WE ARE DOING ABOUT THIS AGE ASSURANCE CHALLENGE** — it's not enough for us to just do nothing and assume platforms are going to take care of it
- ~~Jen to frame the problem! Yeeha — CHAPEAU~~
- Let's really make sure we can handle the feedback/objections that we've seen before
- Figure out the Arkansas model relative to how we probably want to apply the Spotlight Mod flow
- **Get this outcome: Do the spotlight thing it's top priority and also interesting in mixed audience thing after we solve that**
- Mixed audience
 - BIPA consent << dig into more "Is that a valid BIPA consent?" Maybe we do something different in IL and TX
- ~~AO set up weekly time for our crew~~
- Our personal goal is to make this awesome by Thanksgiving
- Add option c — minor birthyear change like IG << we don't recommend this option because it doesn't make sense safety-wise but it's a way to throw a bone to regulators
- Add option d — we can do appeals on U13 deletes << it actually makes us look horrible and is a trap

Age Verification Appeals for U13 accounts via Spotlight Moderation

Our Spotlight Moderation workflow includes human review for every piece of content that receives a large number of views, yet we are currently not directly escalating potential U13 accounts via this workflow due to operational bandwidth limitations on the T&S side. Earlier this year, [TikTok was fined by the ICO for £12.7M](#), estimating that it allowed over 1 million U13 UK children to use TikTok without parental consent in 2020 — the gist of the argument was that because of their moderation practices, TikTok should have been aware that they had all these underage users but did nothing about it. Upon learning this, we conducted an experiment to assess the volume of potential U13 escalations via our Spotlight Moderation workflow and escalated between [2,000-3,000](#) Snaps per day globally. This is a meaningful gap and, based on the ICO/TikTok case, means we are exposed to risk.

There are multiple ways to address this gap, including simply increasing the staffing on our Trust & Safety team dedicated to age verification; however, this workflow is complex and not our core competency, plus several vendors are emerging as leaders in this space. Therefore, this is a compelling opportunity to utilize an age assurance vendor.

Regarding the experience, when a Spotlight moderator observes an account that could be U13, we could suspend the account and give the user 30 days to appeal the suspension by verifying their

age. We'd integrate with Yoti and ask the user to verify their age by taking a selfie or providing ID verification. We'd send the information to Yoti, who will respond as to whether or not the user is under 13. Once verified, the account is restored, and the user can continue to use Snapchat normally.

There are other good reasons to pursue this approach. Based on expected volumes, we could validate the efficacy of third-party age assurance vendors for ~\$100K in 2024, with a part of the overall experience that will not impact our core business. Also, from a regulatory perspective, Spotlight is a significant safety risk since users can quickly achieve enormous reach.

Even if done well, there are risks with this approach. For example, regulators might use our "small experiment" against us and demand that we expand our usage of age estimation tools to other, more consequential parts of Snapchat. While this is a possibility, since respected regulators like the eSafety Commission have officially shared concerns about age assurance technologies, we genuinely believe there is an openness to an honest conversation about what can and cannot work. Without actual data, we can't legitimately participate in that conversation.

to the Camera, Lenses, Memories and the ability to Save to Camera Roll . The second involves adding an appeals process within our existing Spotlight moderation flow and for under 13 deleted accounts that would give these accounts the option to verify their age and continue using Snapchat.

It doesn't make sense that we let people observe driving for 16 years and then they can drive but we think keeping people off the internet and then putting them on with no training is the right way to do it

Key points about the landscape:

- The way almost every app gathers a user's age is through self-reported age, but it is widely assumed that younger people are savvy and know how to misrepresent their age. This is very likely the case both for U13 users and 13-17 users, who misrepresent their age as 18+ to access age-gated features.
- Lawmakers and regulators are most concerned with age assurance for minors, and we've heard first-hand from regulators that they perceive Snap as a high-risk platform because of the prevalence of U18s using Snapchat.
- Other tech companies are already investing in various methods of age verification. For example, TikTok offers four distinct ways to verify age, and Instagram, Messenger, and Facebook use multiple forms of identity verification and facial estimation as part of various age assurance flows ([see here for details](#)). The most common are requiring age verification for U18 users to change their age or providing an appeals mechanism with age verification when accounts are terminated for being U13
- While most regulators are primarily calling for two alternatives to self-reported age (identity verification or parental consent¹), there is no consensus on which approach is best. For

¹ Note parental consent is already an explicit requirement under the GDPR when companies rely on 'consent' as their legal basis for processing data of users who are younger than 16, this is why we try to avoid relying on consent, e.g. in the My AI use case.

example, Australia's eSafety Commission has formally published papers ([here](#) and [here](#)) expressing doubt that these approaches will be feasible, equitable, or secure (a summary is [here](#)).

- Third-party vendors are taking the lead with identity verification/age estimation, but there are open questions about how practical, effective, and privacy-safe these approaches are. Even according to [its own data](#), Yoti highlights how age estimation is much more effective for 18+ vs U18s.
- There are several options for parental consent, but most legislation does not specify the required methods. Commonly accepted ways to do this are through email consent, a toll-free phone number for a live conversation, and using verification via parental control features (the detailed list is [here](#)).
- At least in the recent Arkansas ruling, the court posited the metaphor that you don't get carded when you enter the mall, you get carded when you enter the bar in the mall. This reinforces the principle that we should consider applying age assurance measures when users engage in specific areas within the app that could present some risk to minors (e.g., watching 18+ content) vs when they just enter Snapchat generally (e.g., in registration)

Unlike other products in our general category, we don't currently have any ways to do age assurance. Not only does this expose us to regulatory risk and scrutiny (we'll explain that more below), but it also makes our input to regulators less valuable because it has little basis in real data. And despite being for a general audience (i.e., 13+), our data is also not believable relative to our scale (we delete ~50 U13 accounts per day when other platforms report removing [20 million accounts per quarter](#)). Given our status as the premiere communication tool for minors, this puts us in an especially tough position and makes us a high-priority target for regulators.