



Age Management Escalation

MEETING OVERVIEW

- **TL;dr:** *The primary focus of this meeting is to determine whether and how to link accounts for the purpose of enforcing age across the FB Family of Companies. We hope to align our approach on this topic and prepare for a meeting with Mark on 10/14.*
- **Date/Time:** Tuesday, October 8th, 2:00pm- 2:30pm
- **Location:** Wood for the Trees
- **Attendees:**
 - Joel Kaplan, Erin Egan, [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] Karina Newton, Antigone David and Victoria Grand
- **Attachments?** Pre-read, Age Management Strategic Plan and Age Gating Guidelines attached
- **Precursor to a Mark or Sheryl meeting?** Yes. There will be a meeting with Mark on October 14th about this issue.

GOAL

1. Align on level of priority of proactive enforcement
2. Prepare for MZ discussion on cross-app enforcement

RECOMMENDATIONS

1. PROACTIVE ENFORCEMENT -- How important is it that we proactively enforce based on age (i.e., try to detect and challenge people lying about their age)?
 - a. Background:
 - We have recommended that, by 2021, we use machine learning models to proactively enforce if we believe a minor (<13) is falsifying their age. This is one of the main areas of concern we've heard from regulators/policy makers, and it is more likely to drive concern in the near term than questions about how we enforce across FB/IG/WA.
 - While there is consensus that we should pursue proactive enforcement, the Integrity team is concerned about limited resources and is asking for guidance on how the policy team prioritizes this against other priorities.
 - The Product Policy team previously prioritized areas for Integrity work.
 - Age enforcement could fall under "Authentic Age: False DOB" (which is listed as low severity) or "protection of minors" (which

includes removal of minors based on user request and is listed as very high severity).

- Even with a “very high severity,” at current staffing Integrity estimates this would not be worked on until late 2020 or 2021 at the earliest and would require a substantial investment.

b. Recommendation:

- i. We agree with the Product Policy team that this issue should be classified as “very high severity,” but need guidance on how to rank against other policy priorities.
- ii. Proactive enforcement is our most important policy goal in this area -- so although there’s substantive agreement we should do this we recommend flagging for Mark that it’s not currently staffed and asking for additional resources to support this work in 2020.

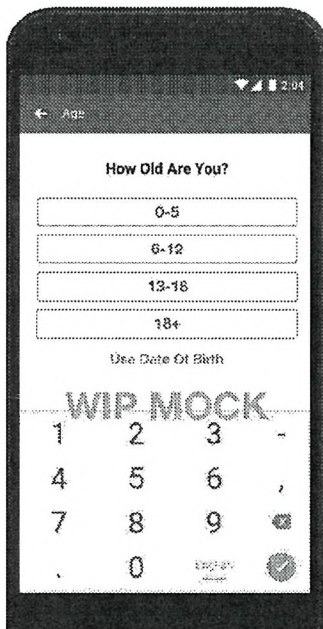
2. CROSS-APP ENFORCEMENT -- If we enforce against a FB account for being underage, under what circumstances should we enforce against IG/WA accounts that we believe are co-owned?

a. Background:

- In the meeting with Mark, the product team will present 4 options for discussion in response to the question, “What sort of account link will we use to enforce?” The primary differentiator is on what the user sees and how this interacts with the rest of the product (i.e., the level of transparency of the account link to the user).
- The options represent short/medium-term solutions for cross-app enforcement of age:
 1. Explicit opt-in account link (with user consent)
 - a. Example: user explicitly connects Instagram account to Facebook account
 2. Implicit, user-driven account link (transparent in the product)
 - a. Example: user cross-posts a WhatsApp status to her Facebook story, but doesn’t explicitly link the two accounts
 3. Inferred account link
 - a. Example: FB and IG accounts used on the same device and we predict they’re likely the same person. This type of inference is often the basis of how we show ads.

4. Opt-out account link from inferred (transparent in settings)
 - a. Example: same as Option 3, but people can opt out of the link
- ii. Recommendation:
 - Option 3.
 - General justification: It is difficult to defend the use of inferred account links for advertising purposes without also using these links for age management
 - Product will likely push back on this by pointing out that the consequences of showing the wrong ad to someone is relatively low compared with the consequence of being checkpointed as an underage account.
 - However, taking this position will invite criticism that we are putting profits over people.
 - Transparency and control: If we are using the fact of an account link for enforcement or other purposes, we recommend being transparent about the fact that this link exists. However, we do not support providing an opt-out of the link because (1) the primary non-ads use of this link is for security and accounting purposes, and we don't want to give bad actors the ability to stop these activities; and (2) there is a separate ongoing discussion about the right control model for cross-affiliate ad delivery that will address this question in the ads context.
 - Application to ads: Note that Options 2 and 3 would allow us to use an inferred link to decide what ads to show on IG, WA, and Audience Network.
 - Long-term, we recommend moving away from the concept of soft-matching -- a practice that is sensitive from a privacy standpoint and also not well understood -- and using tactics like common logins to encourage people to explicitly connect their accounts across services. But we recognize this isn't a realistic option in the near term -- in part because soft-matching is used for a range of purposes, including integrity/security, accounting (total number of users), and ads.

3. [for visibility only] AGE GATING METHOD: How much flexibility do we have in designing the age gate at registration, so that it stops <13s but doesn't block older people legitimately trying to create an account?
- a. Background: Growth is pushing on how flexible our age gating mechanisms can be to mitigate growth impact. The key change we have recommended is changing the default age on FB during registration from 25 to something less than 13. We have also recommended blocking people after their 2nd failure to enter a valid age. Growth estimates an impact of -14M MAP/year on FB and -14M MAP/year on IG [lower confidence estimate].
 - b. Recommendation:
 - i. We've given the Growth team a set of guidelines for what a "gold standard" approach would be for collecting age at registration across FB/IG, and where we see room for variation.
 - ii. The Growth team has asked us to collect external feedback on modifications to allow selecting from pre-determined age ranges (ex. 0-12, 13-18, 19-30, 31-50, 51+), rather than having to specify a specific age.



CONTEXT

We're under increased pressure, especially in Europe and the US, from clients, regulators, and advocates around when/how we should we collect users' ages, and what steps should we take to ensure that what they tell us is accurate. Currently we have a fragmented approach, which is not consistent globally (i.e., EU vs. non-EU) or products (i.e., FB vs. IG); we have been working with product teams to develop a synthesized approach.

Specific decisions:

1. PROACTIVE ENFORCEMENT -- How important is it that we proactively enforce based on age (i.e., try to detect and challenge people lying about their age)?
2. CROSS-APP ENFORCEMENT -- If we enforce against a FB account for being underage, under what circumstances should we enforce against IG/WA accounts that we believe are co-owned?

We also will discuss -- but don't need an explicit decision on -- our AGE GATING METHOD: How much flexibility do we have in designing the age gate at registration, so that it stops <13s but doesn't block older people legitimately trying to create an account?

BACKGROUND

- Background on the issue:
 - We're under increased pressure, especially in Europe and the US, from clients, regulators, and advocates around all aspects of our handling of age. Demands generally focus on 3 main areas:
 - (1) Age of Consent / Parental Consent
 - (2) Age Verification
 - (3) Age-Appropriate Experiences
 - Current approach for age management is fragmented regionally (EU vs. ROW) and by product
- Sensitive issues (recent PR or Policy problems):
 - UK ICO Age-Appropriate Design Code
 - Background: 16 age-appropriate design standards that must be applied to all users in the absence of "robust" age verification mechanisms (e.g., user profiling off by default; ban on "nudge techniques")
 - UK Deep Dive: education on current efforts and challenges of age management, understand UK priorities
 - US FTC
 - COPPA Rule Review: considering application to general audience

- websites with large numbers of u13 users
- YouTube COPPA Settlement: actual knowledge based on child-directed content; creators must self-designate child-directed content
- US Federal & State
 - COPPA 2.0 (Sen. Markey): expands COPPA to u16, bans targeted ads for u13s; “constructive knowledge” standards for COPPA liability
 - California Consumer Privacy Act (CCPA): opt-in for “sale” of minors’ personal info

BACKGROUND ON AFFILIATE PERSPECTIVES

- Policy Position:
 - Ideal Long-term Outcome: Deprecate soft-matching for all purposes and proactively enforce age based on explicit links (i.e., hard-matched accounts).
- WhatsApp Perspective:
 - Comfortable with cross-app enforcement based on stated age for hard-matched accounts
 - Greater concern about -- but likely will not oppose -- use of inferred age for enforcement than level of explicitness for account linking
- Instagram Perspective:
 - Ideal Long-term Outcome: Deprecate soft-matching for all purposes (agrees w/ Policy Ideal)
 - Short-Term Position: Comfortable with inferred account link enforcement, with the understanding that we are working to get to a long-term ideal solution

BACKGROUND ON PROACTIVE ENFORCEMENT BASED ON INFERRED AGE

- Background:
 - CIPCO Policy & CO Comprehensive Violations - This document, prepared by Product Policy, ranks “False DOB” and “Underage Account” as “Low Severity.”
 - Protection of Minors in general is ranked as “Very High Severity.”