

FILED UNDER SEAL

EXHIBIT 21

From: [REDACTED] [/O=THEFACEBOOK/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[REDACTED]]
Sent: 5/8/2021 5:20:01 AM
To: [REDACTED]@fb.com]; Miki Rothschild [REDACTED]@fb.com]; [REDACTED] [REDACTED]@fb.com]; [REDACTED] [REDACTED]@fb.com]; [REDACTED] [REDACTED]@fb.com]; Pavn Diwanji [REDACTED]@fb.com]; [REDACTED] [REDACTED]@fb.com]
Subject: Message summary [{"otherUserFbId":null,"threadFbId":4149822118401578}]
Attachments: 182884695_218552276362806_4637834059085672177_n.png

Pavani Diwanji (5/07/2021 10:34:28 PDT):
>i am writing up a note over weekend to stan/will/adam on u13 and encryption. Any data or research we have that highlights safety concerns > privacy, would be helpful. Any data on existing safety challenges in MK, IG would be helpful. Any research on user perception of the safety/privacy tradeoff will be good to understand. Again I am only asking for research already done that might be avail. If its too much to ask on a friday, please also push back.

(5/07/2021 10:37:17 PDT):
> [REDACTED] on MK UXR just posted new research findings from her work with parents. Here is a link to the E2EE work. <https://fb.workplace.com/groups/MKResearchFYI/permalink/744375159776674/>

(5/07/2021 10:40:12 PDT):
>The other new summary of findings are at the top of this group.
<https://fb.workplace.com/groups/MKResearchFYI> Please let me know if this is what you had in mind.

Pavani Diwanji (5/07/2021 10:43:02 PDT):
>pls chime in with key insight, when you share here, so i understand what tl,dr was at a glance - it would be helpful

(5/07/2021 10:44:39 PDT):
>Adding here since she's the expert on this from the IG data side

Pavani Diwanji (5/07/2021 10:45:18 PDT):
>Context here - there was decision made to encrypt all private messages for u13. This has severe impact on safety as we know. I am trying to argue, perhaps foolishly, that its not the best decision for our users.

Pavani Diwanji (5/07/2021 10:45:27 PDT):
>Decision was made a while ago.

(5/07/2021 10:47:05 PDT):
>The summary of ██████████'s study is:
>> Parents are not technology, privacy, and safety experts. Even if they have heard of end-to-end encryption, their impressions are often uninformed and influenced by the information provided.
>In deciding whether to include end-to-end encryption or not in Messenger Kids, a recommended approach is to select with experts what keeps children of this age group the safest (the core parental need/concern) and then to educate parents on our adopted approach.
>
>But her post is a lot more comprehensive.

(5/07/2021 10:47:29 PDT):
>Also sharing some relevant points the team has made here: <https://fb.quip.com/odPgAKJhbbye#aFNACApAujj>

(5/07/2021 11:06:16 PDT):

>1. Parents are concerned about the privacy and safety/appropriateness of messaging in apps that 6-14 year-olds use.

>2. Parents do not have the technical definitions of privacy and safety used in our industry. At the core of their privacy concerns is safety. First and foremost, they want their children to be safe when using messaging apps and not exposed to inappropriate content.

>3. When asked who is most responsible for keeping their children's messaging private and safe/appropriate, the highest percentage of parents select the app manufacturer for all but the safety/appropriateness of sent messages.

>4. Parents also hold themselves, other parents, and those who use the messaging app responsible for messaging privacy and safety/appropriateness for their children.

[REDACTED] (5/07/2021 12:26:39 PDT):
>Alos, many parents have never heard of end-to-end encryption. Regardless, they have positive impressions of it before reading about it for both children's messaging privacy and safety.

(5/07/2021 12:29:24 PDT):

>Also, Many parents have never heard of end-to-end encryption. Regardless, they have positive impressions of it before reading about it for both children's messaging privacy and safety.

>

> Learning about end-to-end encryption increased the percentage of parents who thought it made messaging less safe/appropriate for their children to where impressions on this dimension across parents now diverged.

>

>Half of parents thought end-to-end encryption should be in Messenger Kids. Those who understood the end-to-end encryption description were less likely to think it should be in Messenger Kids than those who did not understand it. It may be that some parents think Messenger Kids would be safer with end-to-end encryption because their monitoring is sufficient, whereas others prioritize company monitoring.

[REDACTED] (5/07/2021 14:48:35 PDT):

>@Hitomi Hayashi-Branson, I think you have recent IG research to share here, and @ [REDACTED], you may know of any research already done that'll be helpful here, thank you!

[REDACTED] (5/07/2021 14:53:17 PDT):

> [REDACTED], anything else you would like to add from your recent work?

[REDACTED] (5/07/2021 14:55:01 PDT):

>To help make the business case, greater parental satisfaction with Messenger Kids safety features was associated with significantly more invites sent from the Parent Dashboard and higher engagement for tweens. Interestingly, parents' safety over privacy attitude predicated more kid friends for their child on MK. Safety attitudes also impact parents' behavior on Facebook -- specifically, more weekly posts by parent on FB, more time spent on FB, and higher L28 (more days using the app in the last 28 days). [https://fb.workplace.com/notes/\[REDACTED\]/does-the-influence-of-parents-safety-sentiments-on-parent-and-child-online-behav/156840188867300/](https://fb.workplace.com/notes/[REDACTED]/does-the-influence-of-parents-safety-sentiments-on-parent-and-child-online-behav/156840188867300/)

[REDACTED] (5/07/2021 14:55:22 PDT):

shared: 182884695_218552276362806_4637834059085672177_n.png

[REDACTED] (5/07/2021 14:59:09 PDT):

>Messenger Kids is the app most kid users believe keeps them safe when they use it.

>

>TikTok and Snapchat are at the opposite end of the scale, with only 1/3 of kids feeling that those apps keep them safe while using.

[REDACTED] (5/07/2021 15:01:52 PDT):

>MSGR user research from November 2020 also shows how privacy and safety sentiment drives trust/brand sentiment. As safety sentiment goes up, MSGR trustworthiness goes up and nearly *doubles the odds for engagement.* https://docs.google.com/presentation/d/1jopT7ytPcn0NAyC-XtOCix3Yw67H0Dki15PeY-uHm04/edit#slide=id.ga8344e5ea5_0_31

[REDACTED] (5/07/2021 15:02:55 PDT):

>MSGR user research from November 2020 also shows that while performance reliability and privacy sentiment marginally improve the odds that a user will be highly engaged over the odds of not being as engaged (by 1.3x), *safety sentiment has a stronger influence, nearly doubling the odds for engagement.* https://docs.google.com/presentation/d/1jopT7ytPcn0NAyC-XtOCix3Yw67H0Dki15PeY-uHm04/edit#slide=id.ga8344e5ea5_0_31

[REDACTED] (5/07/2021 15:04:09 PDT):

>Parents and kids are in agreement about the importance of safety.

>

>They are also relatively aligned about elements that parents should have complete control over, with contacts and content taking the lead.

>

>Kids of all ages have regular conversations with their parent(s) about online safety, with little variation by age.

>

>Safety is clearly one of MK's major USPs.

[REDACTED] (5/07/2021 15:54:54 PDT):

> [REDACTED] you summarized the E2EE research well. To reiterate, some key points are that:

>• Parents don't think of safety/privacy as we do. At the of the day, they want a messaging experience for their kid that is safe and with appropriate content. When they cite privacy concerns (such as child sharing PI), they really are in the context of keeping their kids safe.

>• Parents say the app manufacturer is most responsible for the safety/appropriateness of child's received messages and to some extent responsible for sent messages as well.

>• Parents don't know what E2EE is, don't understand it, and just think it sounds impressive.

>• After they learn about it and hear some pros/cons, they now are mixed as to whether they think it makes the app more/less safe for their kids. If they understand E2EE after reading a brief description, they are more likely to think adding E2EE makes messaging less safe than those who do not.

>• I think the first two bullets are most important, as E2EE is misunderstood and how you communicate it affects people's impressions.

>Other evidence supporting not using E2EE for our age range:

>• [REDACTED]'s research showing safety is a core MK value proposition.

><https://fb.workplace.com/photo/?fbid=424815445464528&set=pcb.20601719174532>

>Organizations focused on safety typically are against E2EE for children (e.g., National Center for Missing and Exploited children; <https://www.missingkids.org/theissues/end-to-end-encryption>) or at the most take a moderate view (e.g., Unicef).

>• E2EE puts the burden more on parents, who don't necessarily monitor closely.

Pavani Diwanji (5/07/2021 16:01:19 PDT):

>Thanks for all these pointers to wonderful research on MK. Is there IG research? Safety factors in IG direct? Safety in numbers? Thanks

[REDACTED] (5/07/2021 16:25:59 PDT):

>Here's a lit review on private messaging that I'll be sharing widely next week. While additional research might reveal some MK-specific nuances, I'd be surprised if parental attitudes differ significantly from these genpop findings.

>

>A couple of key findings:

>1. Consumer understanding of e2ee is low, so attitudes are highly malleable to the context provided for e2ee. In the end, people want both privacy and safety and don't have the technical knowledge to have a well-defined POV on the tradeoffs.

>

>2. Privacy attitudes vary by individual much more than they do by app. In other words, if someone is concerned about a specific privacy problem on one messaging app, they're likely to be concerned about that same privacy problem on every other messaging app as well.

>

>https://drive.google.com/file/d/1cNGn31_Qm1_v13Vg3Lzhk_cP4XrWAID5/view?usp=sharing

[REDACTED] (5/07/2021 16:28:19 PDT):

>There's also evidence that consumers use the terms "privacy," "safety," and "security" interchangeably. We shouldn't expect them to use this language with the same nuance and specificity that we do internally.

[REDACTED] (5/07/2021 16:34:36 PDT):

>I will say that I'm a bit confused by arguments that e2ee prohibits parents from having visibility and control over the conversation. Since we'll soon be able to encrypt groups, this seems like a problem that could be easily solved by adding the parent (or a parent bot or...) into the conversation. I don't understand why FB would need access to the conversation to enable robust parental controls. So, personally, proactive scanning is the more compelling argument for limiting e2ee in MK.

[REDACTED] (5/07/2021 17:34:40 PDT):

>Here's @Hitomi Hayashi-Branson's hot off the presses IG safety research drawn from interviews with external child safety partner orgs to answer the question what is top of mind and what can we do to make a difference?

https://docs.google.com/presentation/d/1Tau3eZBpIZAluBgmYZ3oacaAxwXXDNyhZYivGO1N9Yw/edit#slide=id.gc8e93b8b3f0_55

[REDACTED] (5/07/2021 17:40:01 PDT):

>Internal child safety data analysis found that the daily number of minor victims having sex talk conversations in IGDM with adults is *38x compared to FB (~200k victims/day).* When normalized for the number of teens, the relative prevalence on Instagram compared to Facebook is about 5x. Original post is here: <https://fb.workplace.com/groups/135709743752034/permalink/624917758164561/>

[REDACTED] (5/07/2021 18:07:24 PDT):

>[REDACTED] mentioned something in today's brainstorm about most of what we catch is through proactive scanning on mk not report. Do you have data on that?

Vaishnavi Jayakumar (5/07/2021 18:11:40 PDT):

>Big fan of @Hitomi Hayashi-Branson's research on IG teen safety that just wrapped up, where she interviewed several of our expert child safety organisations around the world. One of the key findings around both comments and DMs: Children are regularly exposed to sexualising content and comments - girls in particular have come to just expect that they're see this type of content and have these experiences. https://docs.google.com/presentation/d/1Tau3eZBpIZAluBgmYZ3oacaAxwXXDNyhZYivGO1N9Yw/edit#slide=id.gc8e93b8b3f0_1177

>

>As a supporting anecdote, another IG researcher who was recruiting teens for a messaging study met a potential recruit who described a predatory grooming message she received from an older man. The potential recruit was disturbed by this but also mentioned that she regularly gets these kinds of messages, usually at least once a day. That WP post here:

<https://fb.workplace.com/groups/igwb.feedback/permalink/5537311319650771/>

>

>Beyond child exploitation, even adults on Instagram struggle to deal with racist abuse and harassment in their DMs. We just saw a large five-day social media boycott of Instagram by sports clubs in Europe, largely due to footballers and athletes of colour receiving terribly abusive messages in their DMs. Here are a few examples (warning of strong abusive language) outlined in the press: <https://www.the-sun.com/sport/premier-league/812766/ian-wright-racist-abuse-instagram-police/> u-13 children will be even more vulnerable to and impacted by this abuse if they receive it in encrypted DMs, and may not be as well-equipped to report this content to us.

>

>Here's another slide show of the types of abusive messages people receive in their Instagram DMs:

<https://www.instagram.com/p/CBQKovIAS5I/>

>

>I came across this a while back and it's more about Messenger than IGD, but it's research on why people are hesitant to report abuse in their private messages (which is the only way we'd be able to act on such content in an e2ee environment): concerns that reporting is not anonymous, victims not trusting authority, wanting to monitor their abusers / harassers
https://fb.workplace.com/permalink.php?story_fbid=752537048529224&id=100013188075337

Hitomi Dolly Hayashi-Branson (5/07/2021 19:52:16 PDT):

>@silent sorry just catching up here. Thanks Vaishnavi J and [REDACTED] for adding my research with partner organizations. Pavni please let me know if you have any question on this research.

Hitomi Dolly Hayashi-Branson (5/07/2021 22:20:01 PDT):

>@silent Also, please note that this deck summarizing research with external partner organizations (<https://docs.google.com/presentation/d/1Tau3eZBpIzAluBgmyZ3oacaAxwXXDNYhZYivGO1N9Yw/edit?usp=sharing>) has not yet been approved for sharing outside of individuals and closed groups.