

AMENDED Exhibit 261

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

Past Privacy Research at IG and FB: The Evidence Supporting Smart Defaults

MONDAY, 1 JULY 2019 · READING TIME: 18 MINUTES

Goal of this note

To summarize what we know about privacy, security, and safety on Instagram and explain why **Smart Defaults** are a good move.

What are Smart Defaults? - Packaged privacy and security settings that **match users' needs across populations and scenarios**. The goal of creating default packages is to make it easier for users to leverage and benefit from existing privacy and security tools so they can feel safe on Instagram. Ultimately, this will help people experience the best Instagram experience with little effort, including Well-being considerations (Safety, Support).

Key definitions: Security - account access and use, Privacy - account content and interaction

Special thanks to researchers and reviewers: [REDACTED], [REDACTED], [REDACTED], [REDACTED],
[REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED].

TL;DR:

- **Privacy and security are important to users.** Concerns about privacy prevent people from sharing and make it more likely for some users to churn.
 - What are users' main concerns across experiences and how can we empower users?
- **Most users don't know about the tools we have...**And are not likely to go into settings to find them.
 - How can we educate users about our existing tools?

- How can we make these tools more accessible and easier to use?
- How can we promote use of these tools at the right time?
- **Users who do leverage privacy tools are more likely to feel supported.**
 - Do feelings of support differ across different scenarios and use cases?
 - What are other positive outcomes?
- **Users need different sets of controls for different scenarios/use cases.** For example - According to past research, concerns among Indian women are driven by the fear of unwanted contact, photo misuse, and the prevalence of fake profiles, while concerns in Japan are centered on how users' content is being shared.
 - What should these control look like?
 - How would this differ based on user concerns and use cases?
 - How would this differ based on the purpose of the account (e.g., production, consumption, networking, business, a mix of purposes)?
 - When and how should we surface them?
 - How should they evolve with users (and their needs)? For example: I'm a first time user that just got my first IG account and I want a public account so I can build/grow my graph **versus** I'm an established and active user and I want to better refine content I see and people I interact with.
 - How can we educate users on what each package accomplishes without overwhelming users?
- **FB has explored solutions for vulnerable populations** including teens (Fox/Private mode) and women in India (Locked Profile (LP) that allow users to create safe spaces and protect their photos and profile from strangers, respectively.
 - Are there particular vulnerable populations or high risk situations that we should design for?
 - What other solutions can we develop that involve separate spaces or packaged tools?

Questions

- What set of tools are the right ones?
- Will be focus more on populations? Scenarios/situations?
- How can we educate our community about the tools we have as we start building more?
- How can we better educate our community on how these tools work?*

- How can we surface them in a way that promotes awareness and use?
- How can we address perceived negative outcomes from using existing tools such as missing out or social consequence.

For a proposed framework for Facebook privacy education, refer to: Giving the GIFT of Privacy Education (POC: [REDACTED])

How do users define Safety, Privacy, and Security?

Internally, safety, privacy, and security have distinct definitions. According to Facebook research:

- **Safety refers to** physical protections from harm. Relevant tools on FB: Safety Check to broadcast a person's physical well-being to their friends and family in the face of crisis.
- **Security refers to** digital protections from online threats (e.g., compromised accounts, fake accounts, hacking). Relevant tools on FB: the Security Settings menu offers users tools to keep their accounts safe from malicious accounts.
- **Privacy refers to** protections against unwanted observation by other entities. Relevant tools on FB: tools like Privacy Checkup.

However, this is very different from how users describe this. In fact, according to users...

There is no difference. From research with compromise victims to fake account reporters to teenagers in Vietnam, we've found across contexts, continents, and domains of knowledge that people conflate safety, security, and privacy. When we ask about security sentiment, people praise Privacy Checkup; when we ask about Security Settings, they refer to controls only accessible via Privacy Settings; when we ask users' favorite security tools on our platform, 7% of people point to Safety Check.

These are in alignment with findings included in a summary of H1 findings across FB Inc research studies:

'Privacy' is a broad concept. When we ask people to describe the privacy concerns they have across our apps, they respond with a wide variety of topics including data collection, data use, audience controls, how other people are able to interact with them, or more specific versions of each of these topics (see the figure below, which maps out the universe of user privacy concerns) [2].

Security also has a very wide meaning to users. According to Facebook research:

2. A "security scare" encompasses anything out of the ordinary

People feel threatened by a wide range of experiences, some of which have nothing to do with security. Last fall, we asked people to use Facebook as they normally would over the course of two weeks. During that time, they logged screenshots and videos of any experience on our platform that made them feel particularly threatened or unsafe. Results from this research gave additional evidence to a theme we've observed across many qualitative and quantitative studies: People feel threatened by a wide range of experiences, many of which are not related to security at all.

Resources

- What is the difference between safety, security, and privacy? (POC: [REDACTED])
- 7 ways users think about their security (POC: [REDACTED])
- Privacy insights: A synthesis of research and data from H1 2019 (POC: [REDACTED])

Privacy and security are important to users

...And feeling a loss of control is one of the primary drivers behind people deleting or deactivating their Facebook accounts and control takes many shapes (feed, time spent, notifications, and privacy settings).

Users want to feel safe

In a research study on US Tweens and their social media use tweens were concerned with their safety online and were particularly aware of stranger-danger and bullying online. And while they did not seek out trouble, they were aware that trouble could find them. In this

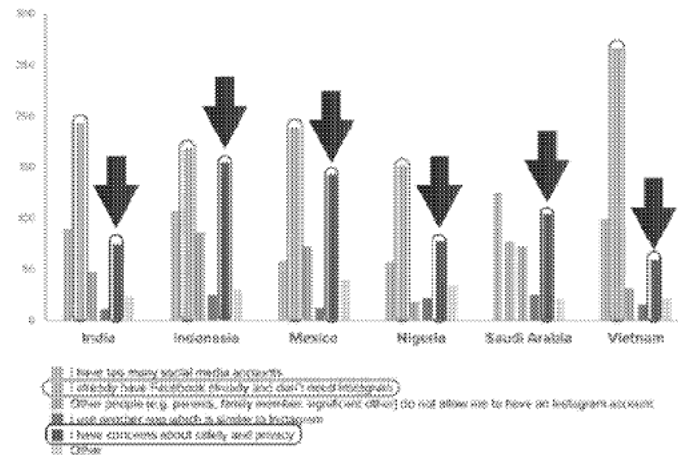
study, parents had similar concerns around privacy and bad actors. There findings were echoed in a research study on the experiences of bullying and harassment among IG users

Users want more control over who can see and interact with their content

In a review of past work on the motivations and barriers to joining Instagram, safety and privacy concerns were key reasons why people were not using IG.

NON-USERS

App redundancy is a consistent barrier across emerging markets, as well as safety and privacy concerns.



This image was edited from the original to highlight concerns about safety and privacy

Research on people who deleted or deactivated their FB accounts showed that negative life impact and not enough control were primary reasons for deleting or deactivation accounts.

Primary reasons for D&D were tied to negative emotional impact and too much time spent overall.

Coded Reasons for D&D

	Privacy	Distraction	Trust	Total
Negative emotional impact	21	6	3	31
Distraction/too much time	7	17	0	24
Privacy concern	12	0	0	12
Trust with personal data	3	4	0	7
Family/friend/relationship drama	5	4	0	9
Social comparison	9	2	0	11
Refresh/report/SUMA*	7	3	0	10
Less relevant	3	1	0	4
Business ethics	5	0	0	5
Harassment/bullying	2	2	0	4
Commerciality	1	1	0	2
				140

1. **Negative emotional impact** is about negative sentiment/content that puts them in a negative state of mind or is emotionally draining.
2. **Distraction/too much time** is mentioned in the context of not being present for family/friends, being distracted from work/school, or feeling that they are wasting time overall on FB.
3. **Privacy concern** is usually uneasiness about who sees their posts, particularly if children are involved. This also includes getting invites from people they don't know.
4. **Trust w/personal data** is often about being hacked or not being sure how/where their information is being used (e.g., personal content used to generate ads).

 Coded from 42,106 open-ended responses to "What's your biggest concern about Facebook?"
 coded per 100,000 responses. (n=100,000 responses)
 Note: Totals may not equal 100% due to rounding.

Facebook App Research 7

In market research studies on how users talk about safety on Instagram - Users were concerned about privacy and control related to control over their content and information (including hacking) and were also concerned about receiving unwanted contact (primarily via direct). For more on hacking and how and when users think about account security, refer to: Account Security - 2 years of research across FB Inc. and IG Privacy & Security Survey: Analysis of open-ended responses (POC: [REDACTED])

- On a personal level, users worry most about **privacy** and **control** over their experience. This includes:
 - The loss of control over content that they own, often by someone they know
 - Unwanted contact, particularly within Direct

HACKING FITS INTO LARGER CONCERNS ABOUT USERS' CONTROL OVER THEIR INFORMATION



- The key safety issue for the users we talked to was being able to control their own content and information. This included:

- Account hacking (e.g. being hacked by a stranger)
- "Personal hacking" (e.g. people accessing things you wanted to be private, this can be done by parents who take your phone or friends' eyes with your password)
- Permanence of content
- Screenshotting
- Location sharing

PRIVACY CONTROLS

When my account is private, I'm fine
I can choose to have a private account and choose who sees what I share.

HACKING

If someone gets your password, you're pretty much screwed. They can edit and post whatever on your account.

PERMANENCE

Once you post something, it's out there forever. It eliminates privacy; it could be used against you at any time.

SCREENSHOTTING

Screenshotting has become normalized ... so people frequently share images without others' knowledge.

Screenshotting is common.

LOCATION DATA

I never post when on vacation. I want until I am home, so satellites burgle don't know I'm away.

We want to know where our kids are, but we don't want other people to know.

13

In a diary study on experiences on Facebook that made users feel particularly threatened (Background and findings and findings and more findings):

- **Half of these experiences involved account security**, including compromise, exposure to fake accounts and suspicious links, and impersonation, as well as friend-on-friend hacking made possible through automatic login.
- **38% of experiences involved privacy-related concerns**, including fears of ad targeting.
- **14% of experiences stemmed from exposure to community standards violations**, including harassment and objectionable content, on our platform. These experiences were significantly more intense than security- or privacy-related experiences.

In a foundational research study exploring how to make FB more useful for women in India - There were strong negative perceptions of FB held by women and their gatekeepers primarily driven by the fear of unwanted contact, photo misuse and the prevalence of fake profiles.

In a research study on sharing among users in Japan, users felt that social networking spaces were not safe and wanted more control over their content and where it could be shared/seen.

Growth Research

So despite using SNS, why do participants still feel that it is not a safe space?

	Poor audience segmentation	Poor content privacy
<i>Wants</i>	The ability to easily define who they are sharing/posting/broadcasting to online	The ability to control when, and where their content is seen and by whom
<i>Worries</i>	Poor targeting of content could result in mis-judgement or creating negative feeling in others	Concerns around content shared beyond their circle and potentially taken out of context resulting in negative judgement
<i>Hacks</i>	Creating multiple accounts on Instagram and Twitter to control their own audiences	Limits sharing of opinions even in LINE chats. F2f / phone calls are still preferred for nuanced conversations

For more research on privacy and security concerns in India and Japan, refer to: WEM Research Narrative (POC: [REDACTED]) and Japan Research Narrative (Nov 2018) (POC: [REDACTED]).

Resources

- 8 Recent Insights from Growth Research (POC: [REDACTED])
- Talking about safety on Instagram (POC: Wendy Gross)
- <https://fb.workplace.com/groups/1526628687644230/> (POC: [REDACTED])
- Casper: Deleters & Deactivators diary study (POC: [REDACTED])
- Why Aren't Users on Instagram Yet? (POC: [REDACTED])
- MAC to the Future: Multiple Accounts Japan Deep Dive (POC: [REDACTED])
- How can we make FB more useful for women in India? (POC: [REDACTED])
- US Tweens and their social media use. (POC: [REDACTED])
- Bullying and Harassment - In-depth interviews on experiences of bullying among targets and witnesses in LA and Walnut Creek (POC: [REDACTED])
- Other interesting research: Othering Fieldwork with Mexican Immigrants Living in the USA (POC: [REDACTED] and [REDACTED])
- Why Japan is more special than we thought (POC: [REDACTED] and [REDACTED])
- WEM Research Narrative (POC: [REDACTED])
- Japan Research Narrative (Nov 2018) (POC: [REDACTED])

- When do people feel threatened on Facebook, and how intense are these experiences?
(POC: [REDACTED])

Most users don't know about the tools we have...And are not likely to go into settings to find them

Current research shows that the tools we have are hard to find. Instagrammers are often unaware of security and privacy features and don't know where to find this in settings,

In a research study on the setting menu, users were aware of some existing control tools (e.g., story control, blocking, hiding) but...

- very few respondents actually used them
- users were more likely to control content at the content level. In fact, most never actually went into the settings menu
- very few could accurately or confidently describe what each tool did

In a FB research study with street intercepts, users were ask to identify Security Settings in their Facebook settings menu. Only 3 out of 23 people were able to find Security Settings, all of whom initially doubted their ability to do so.

"It was clear that people wouldn't spend the time and energy hunting for these settings had we not asked them to do so. Some stated that 'no, I'm not tech savvy—I wouldn't know how to do this' or even 'This isn't Facebook's fault, I just don't know how to get to this.'" – [REDACTED] (UX Researcher)

Lastly, in a research study on graph management, awareness and discoverability (particularly of mute and remove follower) were low, and users had a hard time describing how existing tools worked.

KEY FINDINGS

- 1 Awareness and discoverability of mute and remove followers is low
- 2 Users who are aware of graph management tools are still confused about how these tools work
- 3 Users don't manage their graphs when they are worried about the social consequences and when it is too effortful

OPPORTUNITIES

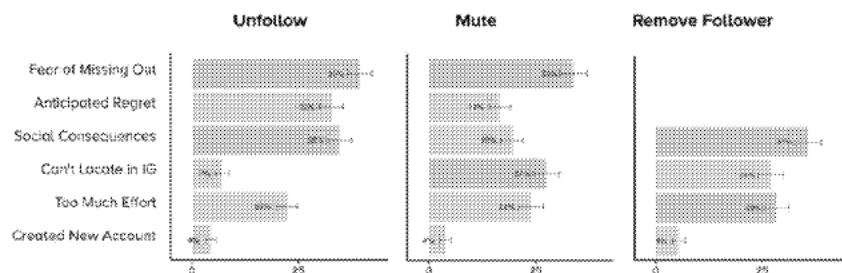
- 1 Should we build a centralized place for graph management tools, in order to increase awareness & discoverability?
- 2 Can we create more targeted education to reduce gaps in knowledge about these tools?
- 3 Should we create a separate tool for tracking relationships, rather than yoking it to decisions about consumption and audience control?
- 4 Can we make graph management tools easier to use (e.g., batching)?

Some users don't want to use existing tools

Common barriers to using existing tools include - fear of missing out, fear of social consequences of taking these actions, and it requiring too much effort.

SUMMARY OF BARRIERS

Unfollow and mute both trigger a fear of missing out. For unfollow & remove follower, users worry about social consequences. All three graph management tools are perceived as too effortful.



These findings are echoed in Othering Fieldwork with Mexican Immigrants Living in the USA where teens were reluctant to take action against bullying even when they had security concerns because they didn't want to be identified as a "tattle" and due to fear of retaliation (online or offline).

Resources

- Settings - Pain Points (POC: [REDACTED])
- Research on settings redesign (POC: [REDACTED])
- Instagram Graph Management in Japan, Brazil, US, & Germany (POC: [REDACTED])
- Othering Fieldwork: IG-relevant Findings (POC: [REDACTED] and [REDACTED])
- How secure do people feel on Facebook? Findings from street intercepts [Compromised Accounts] (POC: [REDACTED])

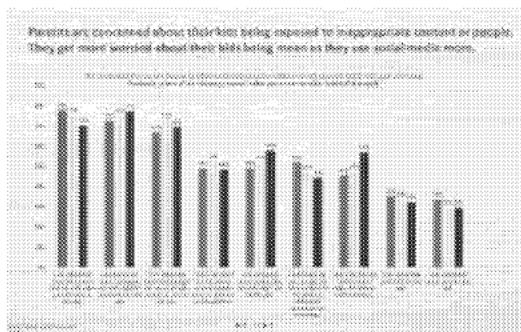
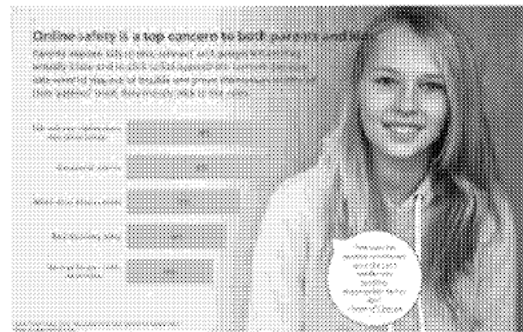
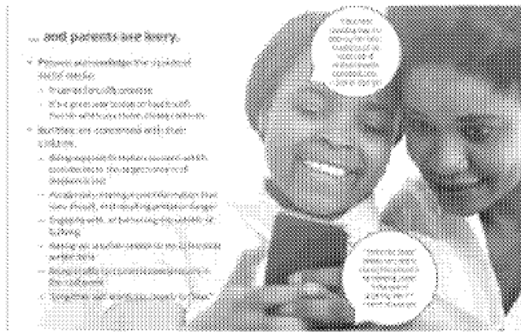
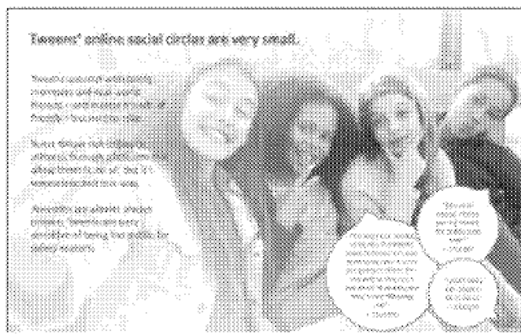
Strategies/tools that users use to feel safe

In a study on multiple account use in Japan, privacy was a top concern among participants. Users developed strategies for managing their anonymity and presence online such as using variations of their names to mitigate discovery by people they didn't want finding them and using Roman characters rather than kanji (Chinese characters) to display their names.

In another study, users were concerned with maintaining a sense of privacy and anonymity for their secondary Instagram accounts. These users protected their identity by using an unidentifiable profile picture and not including their real name in their bio.

In a diary study with a stratified sample of people in the U.S., users indicated that experiences on FB that made them feel safe were related to the discovery and use of tools like Privacy Checkup, Security Checkup, 2FA, and even our Crisis Response feature.
(Background and findings and findings and more findings)

In a research study on US Tweens and their social media use - In order to stay safe, tweens: 1) kept tight circles (friends and family), 2) had private profiles, and 3) were careful with who they followed/friended (and who they accepted as followers/friends) and what they posted.



Lastly, in a research study on the experiences of bullying and harassment among IG users, users who limited their IG network to close family and friends were less likely to have no or fewer experience of bullying. In this study, making their account private (proactively or reactively) and/or using IG less were common strategies to avoid unwanted interactions.

On a related note - Users who control their experience via self-remediation tools report higher feelings of support (for some situations)

In a number of research studies (see resources at the end of this section), self-remediation actions including block, unfollow, or hide resolved the user's problem and make them better after taking the action.

In a survey on what users do when they see objectionable content, blocking and untagging

were associated with feelings of support while blocking was associated with feelings of resolve.

*What factors were associated with feelings of support?**

- While overall feelings of support were low, those with any actioned content in the past 30 days were more likely to feel that IG was supportive
 - Compare to those who did not report anything, those who reported content that was ultimately actioned felt that IG was supportive, while those who reported content that was ultimately ignored felt that IG was not supportive.
- Feelings of support was related to the type of OC
 - Those reporting advertisements, harassment, hate speech, promotion of self-injury, and someone using their photo felt that IG was not supportive.
- Self-Remediation*
 - Blocking and untagging was associated with feeling that IG was supportive.
 - [B/H; n=5,330] Muting and untagging was associated with feeling that IG was supportive
 - [Comment; n= 12,910] Unfollowing and muting was associated with higher feelings of support
 - Using IG less (or stopping for a period of time), selecting to see fewer similar posts, and having to take other actions (not offered by IG) made users feel less supported by IG.

*For more detailed results, refer to: <https://fb.quip.com/codeAMhcVCwL>.

50

*What factors were associated with feelings of resolve?**

- Feelings of resolve was related to the type of OC
 - Those reporting content (e.g., photo, comment, video) as opposed to profile, felt that their issue was not resolved.
 - Those who reported advertisements or promotion of self-injury felt that their issue was not resolved.
 - Those who reported someone tagging them without their permission or spam felt like their issue was resolved.
- Self-Remediation*
 - Blocking was associated with feeling that their issue was resolved.
 - [B/H; n=5,880] Blocking was associated with feeling that their issue was resolved.
 - [Comment; n= 12,910] Blocking and unfollowing was associated with feeling that their issue was resolved.
 - Using IG less (or stopping for a period of time), selecting to see fewer similar posts, and having to take other actions (not offered by IG) made users feel that their issue was not resolved.

*For more detailed results, refer to: <https://fb.quip.com/codeAMhcVCwL>.

51

In a survey study on the experiences of teen targets on Instagram - Overall, blocking was more effective in solving users' issue(s), while spending less time on IG/closing an account,

making their account private/changing privacy settings, and reporting were less effective actions. **But findings were mixed...**

- **across aggression type...** - Actions taken were less effective for exclusions and damages to reputation and were more effective for threats and unwanted contacts. [Damages to reputation was among the most upsetting to users.]
- **and actor...** - With the lowest resolution among those who experienced this from friends, family, and groups of people, and the highest resolution for those who experienced this from strangers.
- **and surface** - With the lowest resolution among those who experienced this on their feed or a hashtag page, and the highest feelings of resolution for those who experienced this on DM. This is unsurprising as the most common aggression type was unwanted contacts via DM by strangers and people expressing romantic interest.

While blocking was very common, it was not a sufficient solution when there were perceived consequences of blocking, they needed to keep an eye on their bully, or they wanted to keep the bully in their lives (mostly for known actors). For more details on when block is and is not the right solution, refer to this document: Bullying experiences: When blocking IS and IS NOT the right solution.

Resources

- Meta-update on the work to understand the value of self-remediation ([REDACTED])
- Why Self-Remediation Matters ([REDACTED])
- Self Remediation (Block, Unfollow, Hide): Are these positive outcomes? ([REDACTED] [REDACTED])
- Why the Support Flow Matters ([REDACTED])
- Why do Instagram users block accounts? A five-country in-app survey (POC: [REDACTED] [REDACTED])
- Why do Instagram users delete comments? A five-country in-app survey (POC: [REDACTED] [REDACTED])
- How users perceive and cope with objectionable content on Instagram (POC: [REDACTED])
- Is Self Remediation (Block, Unfollow, Hide) a 'Positive Outcome'? (POC: [REDACTED] [REDACTED])
- Bullying and Harassment - In-depth interviews on experiences of bullying among targets and witnesses in LA and Walnut Creek (POC: [REDACTED])
- Bullying experiences: When blocking IS and IS NOT the right solution (POC: [REDACTED] [REDACTED])

- Reporting – Understanding what users do when encountering objectionable content (POC: [REDACTED])
- How safe do people feel on Facebook, and what impacts their perception of safety? (POC: [REDACTED])
- What types of experiences make people feel safe on Facebook? (POC: [REDACTED])
- When do people feel threatened on Facebook, and how intense are these experiences? (POC: [REDACTED])

Users need different sets of controls for different scenarios

In a research study on what privacy control features users would want bundled to help them avoid unwanted interactions, responses varied based on situations.

If someone is bullying me I'd want to hide my activity across Instagram. I wouldn't want them to see my status or any of my activity or posts...But if I just didn't want my parents to see what I was doing, i'd just probably want to hide my stories. – Female, Teen

In reporting and bullying and harassment research studies, participants were particularly concerned with protecting younger users.

For kids, there should be some way to limit what they see...so they wouldn't be able to see violence or drugs or other inappropriate things...At the same time there should also be a way to limit who can reach them. – Female, Adult

In this same study, the idea of selecting who can see your activity was brought up many times.

If i'm apply for a job, or I don't want my co-workers and boss to see what I'm doing, it'd be nice to have a way to hide my stories and also make it so they can't see certain posts – Female, Adult

I'm muslim, and there are a lot of people in my community, older people, that don't approve of the clothes that I wear...They'd make inappropriate comments expressing their disapproval...They don't mean to shame me, but I wish they would do it less publicly...It'd be nice to limit what they can see and what they can say on my posts. – Female, teen

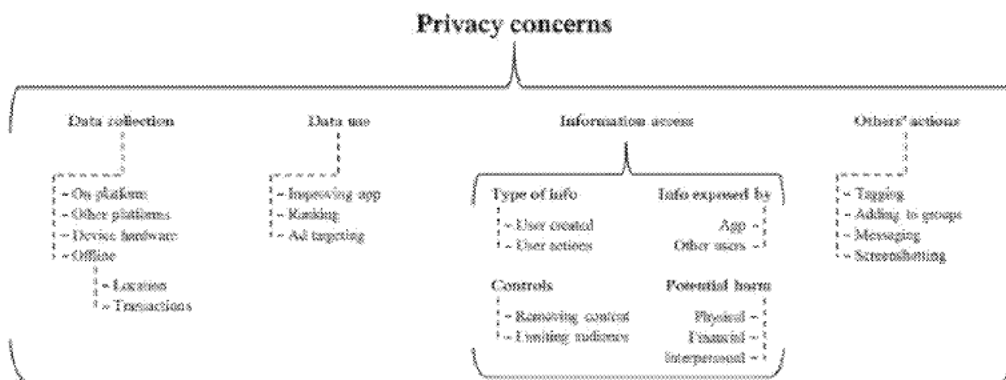
In the above discussed studies on privacy and security concerns in Japan and India, we saw that users' concerns across these different populations varied greatly, thus calling for different solutions (e.g., protecting photos, protecting identity, discoverability).

Lastly, in a summary of H1 findings across FB research studies, [REDACTED] suggest developing options based on use cases.

Insight 3: Focus on a specific use case, not the general concept of privacy

'Privacy' is a broad concept. When we ask people to describe the privacy concerns they have across our apps, they respond with a wide variety of topics including data collection, data use, audience controls, how other people are able to interact with them, or more specific versions of each of these topics (see the figure below, which maps out the universe of user privacy concerns) [2].

Individual privacy features can't address every aspect of privacy (e.g., audience controls have nothing to do with data collection). Additionally, trying to cram too much information or too many controls into a single feature can be overwhelming for some users and make it difficult for them to find what they're looking for. As a result, privacy features that focus on a specific use case will be better able to deliver value. Privacy features should also clearly communicate what elements of privacy they do (and don't) address so users can easily identify whether a particular feature will be useful for them.



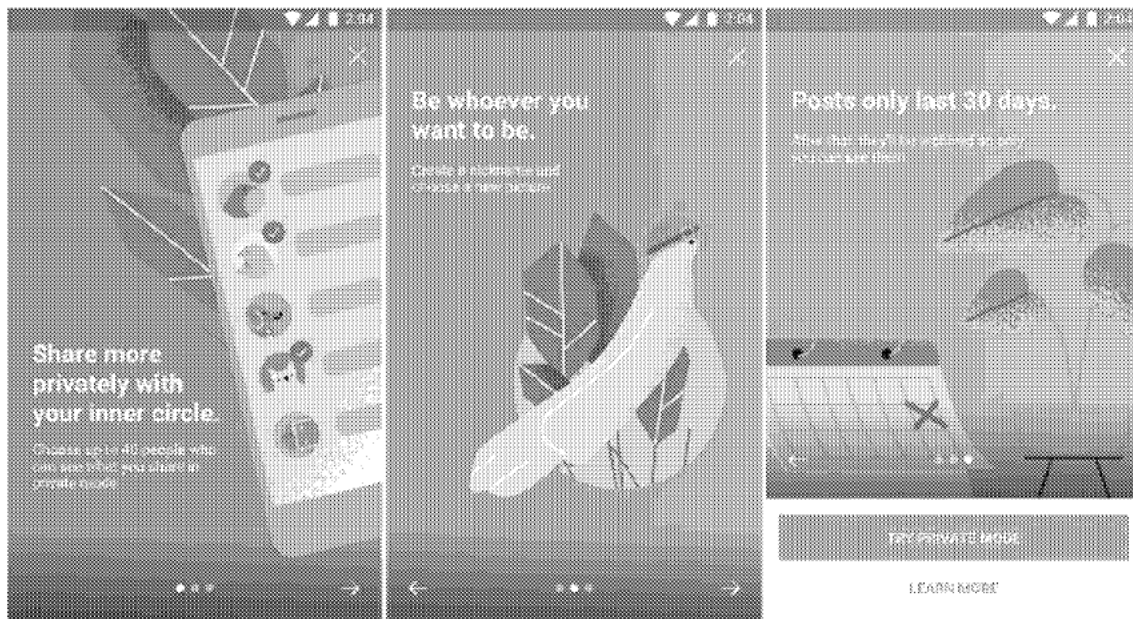
Resources

- Rolling research (3/13) on protected mode (POC: [REDACTED])
- Rolling research (3/13) on the comment reporting flow (POC: [REDACTED])
- Bullying and Harassment - In-depth interviews on experiences of bullying among targets and witnesses in LA and Walnut Creek (POC: [REDACTED])

- Feedback on Restrict - 15APR2019 (POC: [REDACTED])
- Research on settings redesign (POC: [REDACTED])
- MAC to the Future: Multiple Accounts Japan Deep Dive (POC: [REDACTED])
- How can we make FB more useful for women in India? (POC: [REDACTED])
- Privacy insights: A synthesis of research and data from H1 2019 (POC: [REDACTED])

What else have others done?

Fox Mode/Private Mode: A separate space where people can share with a subset of their friends.



What is Private Mode?

Our team believes that privacy and audience control is a significant factor limiting how much teens share on Facebook. Teens feel pressure to accept friend requests from everyone - like relatives - but still want a space to share where those loose ties are not going to see or interact with my posts. Private Mode will help teens directly control who they share with in a clear, understandable way by separating their graph, feed, and production experience into a new space within the Facebook app. And over time, we'll incorporate new fun things to do that make this feel less like a 'bizarro Facebook'.

In Private Mode, teens can share & interact...

- in a completely separate space with its own UI/color scheme, and feed
- with a subset of their friends
- using a nickname...

...so that it feels private, exclusive, and fun.

Due to findings (summarized here and more here) indicating that people were not sharing in Private Mode, even though adoption & visitation retention were high, the community integrity team concluded that pseudonyms + limited audience + separate space by itself cannot significantly drive sharing.

Locked Profile (LP) - a simplified FB privacy feature from our Women in Emerging Markets (WEM) team to address photo safety concerns that is similar to Private IG Accounts.

Context

Problem

1. Photo safety concern is the largest barrier to joining FB for internet users in India, affecting ~23M users¹
2. Post participation gap in India is almost entirely from women, 70% of whom feel somewhat or less safe sharing a photo or video of self on FB²

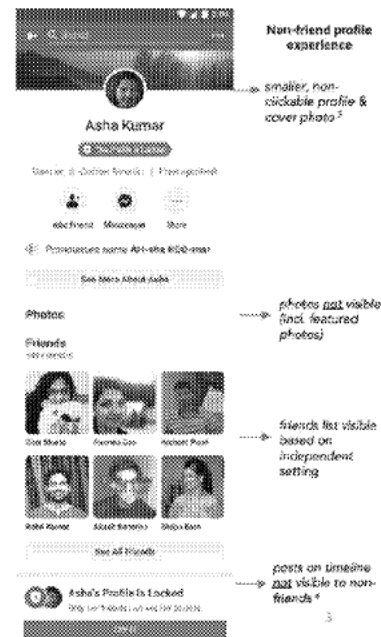
Strategy

1. Make people on-platform feel safer leading to better engagement, retention and acquisition (via referrals and marketing)

Product Solution

1. Account-level, opt-in solution that **prevents non-friends from viewing your photos and posts on your profile**⁴
2. Similar to **Instagram private accounts** which is widely adopted in India
 1. ~35% of India MAP, ~62% India female MAP has a private account on IG

¹ India Barometer Survey, 2017. Numbers are likely higher given growth from 2016. ² On-platform survey measuring photo safety sentiment. Post participation is correlated with photo safety sentiment. ³ Sample includes the users, in the photo, and on their profile (with a restriction on a C-level privacy (eg. 100+). ⁴ This solution is not available in all countries. Please, consult the local legal team for more information. ⁵ This solution is not available in all countries. Please, consult the local legal team for more information. ⁶ This solution is not available in all countries. Please, consult the local legal team for more information.



Research on LP found significantly higher safety sentiment among users with LP than in the control condition, indicating LP increases feelings of photo safety and control among users which we know is a major barrier to WEM.

Resources

- Dogfooding Private Mode (POC: [REDACTED])
- Wrapping Up Private Mode (POC: [REDACTED])
- Locked profile survey in BD pt 1: Safety sentiment in product test v. control (POC: [REDACTED])
- How can we make FB more useful for women in India? (POC: [REDACTED])

Vision for Smart Defaults

Packaged smart defaults that match user's needs across populations and scenarios. The goal of creating these packages is to make it easier for users to leverage and benefit from existing privacy and security tools so they can feel safe on Instagram.

For example, these packages might be designed around different age groups

- Teens
- Adults

...different scenarios/situations

- I'm being bullied
- I'm applying for a job or trying to keep it professional
- I want to have a public account, but I'm worried about unwanted interactions
- I'm a new user versus an established user
- I use IG to network versus to browse versus to post things (etc.)

...special security needs (who may need an extra-high level of security- strong passwords, must have 2FA, etc.)

- Celebrities
- Critical Civic Actors (e.g., politicians, journalists, activists)

Planned research

Research Plan - Smart Defaults (A/V Priv -T46017675)

Goals: To understand different privacy and security concerns and needs across:

- Different populations (e.g., teens versus adults, communities/groups)
- Situations/scenarios/Use cases (e.g., when i'm looking for a job, when i'm being bullied)

19

3 comments 13 shares

Like

Comment

Share

Save



Diego Castaneda

Like · Reply · 31w



Diego Castaneda replied · 1 reply



#thanks [redacted] for the incredibly useful synthesis of Instagram privacy research! It has been super helpful in setting a baseline of knowledge for me.

Like · Reply · 3w



Write a comment...